Entanglement Distillation

A Discourse on Bound Entanglement in Quantum Information Theory

Lieven Clarisse

PhD thesis

Abstract

In recent years entanglement has been recognised as a useful resource in quantum information and computation. This applies primarily to pure state entanglement which is, due to interaction with the environment, rarely available. Decoherence provides the main motivation for the study of entanglement distillation. A remarkable effect in the context of distillation is the existence of bound entangled states, states from which no pure state entanglement can be distilled. The concept of entanglement distillation also relates to a canonical way of theoretically quantifying mixed state entanglement.

This thesis is, apart from a review chapter on distillation, mainly a theoretical study of bound entanglement and the two major open problems in their classification. The first of these is the classification of PPT bound entanglement (separability problem). After having reviewed known tools we study in detail the multipartite permutation criteria, for which we present new results in their classification. We solve an open problem on the existence of certain PPT states. The Schmidt number of a quantum state is a largely unvalued concept, we analyse it in detail and introduce the Schmidt robustness. The notion of Schmidt number is exploited in the study of the second major problem, that of the existence of NPT bound entanglement. We reformulate this existence problem as particular instance of the separability problem, present a uniform treatment of distillability and numerically demonstrate that bound entanglement is primarily found in low dimensional systems.

Contents

List of Figures

Preface

Quantum error correction allows quantum information to be reliably sent through noisy channels. Tremendous effort has been devoted to the study of quantum error correcting codes and capacities of quantum channels. This thesis deals with entanglement distillation, also known as counterfactual error correction [138]. The idea is to purify the noisy channel before trying to send any information over it, rather than the more indirect method of error correction. Personally I feel very strongly about the idea of distillation since it also relates directly to a canonical way of quantifying how much useful entanglement is present in a state. The distillable entanglement is a physical property of quantum states, bridging between a practical and theoretical study of entanglement. Bound entangled states are states from which no pure entanglement can be extracted, although entanglement is needed to construct the state. They are two main open problems in the classification of bound entangled states (the separability and the NPT bound entanglement problem) and they constituted the bulk of my research.

During the course of my Ph. D. I have published a number of papers, but in writing up, I have tried to make this thesis more than just a compilation or medley of these papers. The primary goal has been to convey the context and motivation of the different problems. Secondary, I have tried to provide a review of the state-of-the-art knowledge in entanglement distillation in the bipartite scenario. A notable gap in this presentation is a treatment of experimental entanglement distillation. The structure

of the dissertation and the interrelation between the chapters, is depicted in Figure 1. The figure also contains a reference list of my papers, and their position in the thesis.

Chapter one deals with the separability problem. After having reviewed the theory of positive maps and entanglement witnesses, I present new classes of PPT entangled states with particular ranks. Next, the permutation criteria for separability are studied in detail and a new result on their classification is presented. This is the only place in the dissertation which deals with multipartite systems.

The Schmidt number of mixed states is a generalisation of the separable versus entangled division, imposing a finer structure on the set of quantum states. This is the topic of Chapter two. The tools for the separability problem are readily generalised to deal with Schmidt numbers. I review in some detail known results. In a final section, I introduce the Schmidt robustness and derive upper and lower bounds for pure states. The motivation for the topics discussed in this chapter becomes clear in Chapter four.

In Chapter three I review the literature on bipartite entanglement distillation. After the necessary introduction of quantum operations, the main results on pure state entanglement transformation are sketched. Then I move over to mixed state entanglement. I start with a discussion on entanglement measures focusing on the distillable entanglement and end with a discussion of irreversibility in mixed state transformations. This leads to the introduction of bound entangled states. The chapter ends with a review of mixed state entanglement distillation protocols.

Chapter four is a discourse on distillability and NPT bound entanglement and describes my main results. As usual, the first sections introduce known results. In particular I review the three fundamental theorems on distillability. Next a uniform treatment of distillability theorems is presented. I illustrate the power of this reformulation by means of four applications. The most important ones are the derivation of reduction-like maps and an estimation of the volume of distillable states. In the next section the problem of the existence of NPT bound entanglement is reformulated as the problem of determining whether a particular set of states is entangled. It follows that the two major open problems on the classification of bound entangled states are really just one problem (although the problems are by no means equivalent). I end this dissertation with a short review on activation of bound entanglement.

Figure 1: Structure of the dissertation and publications.

Acknowledgements

Words fall short in gratitude to my supervisor Anthony Sudbery. He took the ungratifying task of agreeing on the supervision of an international student, with little or no references. Subsequently he arranged, together with Samuel Braunstein, financial support. I thank both of them wholeheartedly for this. From the very start Tony has been enormously encouraging and helpful, always making time for me despite a plethora of departmental duties. I have enjoyed many discussions with him; his mathematical quickness and wittiness never cease to amaze and inspire me. It is also hard not to acknowledge the mental support he offered me when I was in need for it the most.

Many thanks go to my coauthors Sibasish Ghosh, Simone Severini, Anthony Sudbery and Paweł Wocjan; it was a true honour and pleasure working with them. During my Ph. D. I enjoyed discussions with a number of researchers, including those who have helped me out clarifying technical issues on their own work. In particular, I want to thank Samuel Braunstein, Ignacio Cirac, Jens Eisert, William Hall, Otfried Gühne, Erik Hostens, Florian Hulpke, Maciej Lewenstein, Andreas Winter and Christof Zalka. I thank Stefan Weigert and Martin Plenio for pointing out numerous mistakes.

My girlfriend Christine has played a vital role in the completion of this Ph. D.; Thank you Christine, for your continuous support, dedication and love. Equally appreciative I am for her commitment during the final year, which was infested by a prolonged period of illness. I would also like to express a deep gratitude to my parents and my brother and his wife who supported and encouraged me throughout. It was my parents financial support during the first year that made my move to York possible. I thank my friends in Catherine House and fellow Ph. D. students for support, friendship and a wonderful time in York.

I enjoyed financial support through a W. W. Smith Scholarship and EPSRC grant GR/S822176/01 for which I feel greatly indebted.

This thesis was typeset with the Miktex distribution (`www.miktex.de`) of LaTeX and text editor Winshell (`www.winshell.de`). The figures were produced using GraphEq (`www.peda.com`), Mayura Draw (`www.mayura.com`) and Matlab (`www.mathworks.com`).

York   Lieven Clarisse

July 2006

Author's declaration

Most of this material has been presented before. This is true for all literature review and most of the original work. The introduction of PPT states with special ranks, Section 1.2.4 has been presented in Ref. [62]. Theorem 1.3.4 is one of the few results that has not been presented before. The new results on the classification of permutation criteria Sections 1.3.3 and 1.3.4 have been obtained in collaboration with P. Wocjan and published in Ref. [63]. The main idea came from myself. The results on the Schmidt robustness have been published in Ref. [61]. In Section 3.1.3 the paper on the entangling power of permutations is briefly mentioned. This paper was written in collaboration with S. Ghosh, S. Severini and A. Sudbery, with me being the first author [64]. The new results in Sections 4.2 and 4.3 have been obtained by myself and published in Ref. [59, 60]. The Appendix contains two Matlab programs, which have not been published before. See also Figure 1 (page viii) for a schematic overview of the published papers and their position in the thesis.

Entanglement and separability

From the 1930s, starting with the EPR thought experiment [27, 88], entanglement was mainly studied in the context of the completeness of quantum mechanics. It was not until the 1960s when the problem of completeness was put on solid mathematical grounds by the remarkable works of Gleason [106], Kochen and Specker [175] and Bell [16, 17]. The work of Bell dealt directly with the EPR thought experiment and is of enormous importance as it showed that entanglement is incompatible with a certain local classical inequality which can be verified experimentally. We will discuss the EPR argument and Bell's inequality briefly in Section 1.1. More in-depth treatments can be found in Ref. [222, 244].

In recent years, the problem of completeness seems pretty much settled and considerable effort has been put into understanding the mathematical structure of entanglement. A primary problem is, given an arbitrary quantum state, to determine whether it is entangled or not. The study of this problem came together with the realisation that Bell-like inequalities are pretty weak tests for entanglement. The breakthrough [132, 223] came when notions from convex analysis and $\mathcal{C}^*$-algebras were applied to the problem. In Section 1.2 we review these mathematical results leading to the general framework of entanglement witness and its dual formulation in terms of positive maps. We also introduce the so-called PPT states and relate them to classical problems in

linear algebra. The separability problem has been shown to be NP-hard [110], and therefore there is little hope of finding a simple analytical method which is able to distinguish all entangled states from all separable. Subsequently, interest has grown in finding good numerical methods in tackling the problem. In Section 1.2.5 we apply tools from semidefinite programming to the separability problem. In particular we focus on the work by Doherty et al. [75], which besides a complete numerical solution, offers appealing analytical features.

In Section 1.3 we step away from the entanglement witness approach and study the permutation criteria for detecting entanglement, initiated in Ref. [251] and further developed in Ref. [44, 63, 144, 254, 324]. Although in general, these criteria cannot detect every entangled state, they are particularly appealing because of their operational simplicity and can be applied in the bipartite as well as the multipartite scenario.

Reviews of the entanglement versus separability problem, from a variety of different viewpoints, can be found in Ref. [37, 39, 84, 85, 138, 184, 263, 283, 284].

1.1   The EPR argument and Bell's inequalities

The existence of entanglement [260] follows naturally from the quantum mechanical formalism. This was first made explicit in the famous paper [88] by Einstein, Podolsky and Rosen (EPR), where it was used to argue that quantum mechanics as a physical theory is incomplete. Their argument runs as follows. Consider a particle with known position decaying into two equal particles. Without measurement, all we know is that the particles will drift apart with opposite momenta and that their centre of mass remains constant throughout. Assuming that both particles are well separated, there is no way a measurement on one of the particles can affect the other particle. This is the famous *local realism* assumption, which dictates that well separated systems can be completely and independently described. Now, measuring the momentum or position of the first particle enables one to predict either the momentum or position of the second system, without disturbing it. In quantum mechanics position and momentum are non-commuting observables and the theory cannot predict precise values for both, hence EPR are led to conclude that quantum mechanics is incomplete. A formidable philosophical debate followed on the foundations and interpretation of quantum mechanics,

starting with Bohr's reply [27]. For a historical account see Ref. [167].

In 1951 Bohm [26] formulated a version of the EPR argument with an entangled spin system. Here both well separated parties (A and B) share one half of the singlet state

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Measurement of the spin of the first half in any direction reveals the spin of the other particle in that direction. By an EPR argument the quantum mechanical description of the second half cannot be complete. It is for such a system Bell [16] derived his famous inequality. We will present here a proof of the more general CHSH inequality [66].

Suppose the two parties share a large number of singlet states and measure them one by one. For each measurement, observer A chooses to measure the spin in direction $\vec{a}$ or $\vec{a'}$ at random (with results a_n or a'_n). Analogously observer B measures the spin of his half in direction $\vec{b}$ or $\vec{b'}$ (with results b_n or b'_n). Let us denote with $Q(\vec{a}, \vec{b})$ the average value of the product of the measurements outcomes ab. This quantity is a measure of the correlation between the two measurement outcomes. Now the EPR argument implies that for each singlet pair, a_n, a'_n, b_n, b'_n have definite values (± 1) before a measurement has taken place. By going through all combinations, it is easy to see that

$$a_n(b_n + b'_n) + a'_n(b_n - b'_n) = \pm 2.$$

Because the left hand side is either -2 or +2, its average over all n is not larger than 2, thus we get on average

$$|Q(\vec{a}, \vec{b}) + Q(\vec{a}, \vec{b'}) + Q(\vec{a'}, \vec{b}) - Q(\vec{a'}, \vec{b'})| \leq 2.$$

This inequality gives an upper limit to the correlation coefficients. Choosing the unit vectors $\vec{a}, \vec{b}, \vec{a'}, \vec{b'}$ in the same plane but separated by angles of $\pi/4$, one can verify that this inequality is violated quantum mechanically for the singlet state (with a value of $2\sqrt{2}$). Bell type inequalities can be derived for any number of parties, for more than two distinct measurement outcomes or for any number of alternative setups, see Ref. [225].

Violation of the Bell inequalities has been experimentally demonstrated using the polarisation of photons [6, 99] and experimental results are in excellent agreement with the predictions of quantum mechanics. Apart from entanglement in polarisation,

violation of Bell inequalities with photons has been demonstrated using entanglement based on position and time [98, 288], phase and momentum [243] and orbital angular momentum [195]. Experiments also have been conducted without the use of photons, namely with protons [180] and atoms [248]. It should be mentioned however, that to date no experiment has been loophole free, so that technically, local realism has not been ruled out experimentally. An example of such a loophole is not having proper time-like separation of the detectors (see Ref. [65, 100] for a discussion of these matters).

1.2 The main road

For any entangled pure state shared by an arbitrary number of parties, it was shown that there exists a Bell inequality which is violated [104, 235]. For mixed states this does not seem the case. In this context it has been shown that although a state might not violate any Bell-like inequality, it still may be useful for teleportation [154, 233]. Other states only violate some inequality after a certain local generalised measurements [105, 234]. Yet other states only show a violation when multiple copies are measured collectively [224]. It will be clear that Bell inequalities are a poor test of non-classical behaviour. It has proven convenient to characterise the set of entangled mixed states with a certain reasonable mathematical definition. The advantage of this approach is to have a workable definition of what is entangled and what not. Though only recently it has been rigorously proven that all states defined in such way behave truly non-classically (see Chapter 4).

We will give the definition of entanglement for bipartite states, generalisation to multipartite states is straightforward. Let us first recall the definition of a pure state [94, 260]. Let $\mathcal{H}$ be a Hilbert space such that $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \cong \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ (with integers $d_1, d_2 \geq 2$). A pure state $|\psi\rangle \in \mathcal{H}$ shared by two parties A and B is called separable if and only if it can be written as

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle,$$

with $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$, in other words, if $|\psi\rangle$ belongs to the Cartesian product $\mathcal{H}_A \times \mathcal{H}_B \subset \mathcal{H}_A \otimes \mathcal{H}_B$ [279]. Otherwise we call $|\psi\rangle$ entangled.

There is a simple way of determining whether a pure state is entangled based on the Schmidt decomposition:

Theorem 1.2.1 (Schmidt decomposition [94, 214, 259])**.** *Let* $|\psi\rangle \in \mathcal{H}$, *then there exist orthonormal states* $|a_i\rangle$ *and* $|b_i\rangle$ *such that*

$$|\psi\rangle = \sum_i \lambda_i |a_i\rangle |b_i\rangle, \qquad (1.1)$$

with $\lambda_i \geq 0$ *and* $\sum_i \lambda_i^2 = 1$. *The coefficients* λ_i *are known as the Schmidt coefficients. The number of non-zero Schmidt coefficients is referred to as the Schmidt rank* $S(\psi)$ *of* $|\psi\rangle$. *The state* $|\psi\rangle$ *is separable if and only if it has Schmidt rank one.*

Proof. Let

$$|\psi\rangle = \sum_{ij} \psi_{ij} |ij\rangle,$$

with $\Psi = \{\psi_{ij}\}$ a matrix of complex numbers. Recall that by the singular value decomposition [126] every matrix Ψ can be written as $\Psi = UDV$, with U and V unitary and D a diagonal matrix with nonnegative elements. So we have

$$|\psi\rangle = \sum_{ijk} U_{ji} D_{ii} V_{ik} |jk\rangle.$$

Now putting $|a_i\rangle = \sum_j U_{ji}|j\rangle$, $|b_i\rangle = \sum_k V_{ik}|k\rangle$ and $\lambda_i = d_{ii}$ we obtain the form (1.1). The orthonormality follows from U and V being unitary. To check whether a pure state is separable it is therefore sufficient to calculate the rank of Ψ. $\qquad\square$

Moving to mixed states, let us denote with $\mathcal{L}(\mathcal{H}, \mathcal{H}) = \mathcal{L}_{\mathcal{H}} = \mathcal{L}_{\mathcal{H}_A \otimes \mathcal{H}_B} \cong \mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B}$ the set of linear operators on $\mathcal{H}$. Since we are working over a finite dimensional space $\mathcal{L}_{\mathcal{H}} \cong \mathcal{M}_{d_1 d_2}$ the space of complex matrices of order $d_1 d_2$. The subset of (Hermitian) positive semidefinite operators will be denoted $\mathcal{L}_{\mathcal{H}}^+$. The set of density operators on $\mathcal{H}$ constitutes then the normalised operators in $\mathcal{L}_{\mathcal{H}}^+$ and we will denote them with $\mathcal{D}_{\mathcal{H}}$ or simply $\mathcal{D}$. A bipartite mixed state $\rho \in \mathcal{D}$ is called separable if and only if it can be written as a convex sum of pure product states, i.e.

$$\rho = \sum_i p_i |\psi_i^A\rangle\langle\psi_i^A| \otimes |\psi_i^B\rangle\langle\psi_i^B|,$$

with $p_i > 0$, $\sum_i p_i = 1$, $|\psi_i^A\rangle \in \mathcal{H}_A$ and $|\psi_i^B\rangle \in \mathcal{H}_B$. Otherwise the state is called entangled. The set of separable states will be denoted $\mathcal{S}$ and can thus be identified

with the convex hull of the normalised operators in $\mathcal{L}^+_{\mathcal{H}_A} \otimes \mathcal{L}^+_{\mathcal{H}_B} \subsetneq \mathcal{L}^+_{\mathcal{H}_A \otimes \mathcal{H}_B}$. If such a decomposition exists, then from the Caratheodory theorem [146, 247] follows that we can always replace it with a decomposition of at most m^2 terms where $m = d_1 d_2 = \dim \mathcal{H}$. This definition was first coined independently by Werner and Primas in 1983[1], but popularised in Ref. [321]. The physical idea behind it is that a separable state can always be constructed by two independent parties with the aid of classical communication only (but again, a full physical justification came first later).

1.2.1 Hahn-Banach theorem and entanglement witnesses

To check whether a pure state is entangled it is sufficient to expand it in its Schmidt decomposition. For mixed states the problem is much harder as no such canonical decomposition can be obtained in a straightforward way. However, by exploiting the convexity of the set of separable states a useful characterisation can be obtained, which we will use to construct some necessary conditions for separability.

The following theorem gives a geometrical characterization of the problem of determining whether $\rho \in D$ is contained in a certain convex subset $C \subset D$:

Theorem 1.2.2. *Let $C \subset D$ be a convex set of states in a Hilbert space $\mathcal{H}$, then for each $\rho \notin C$ there exists a Hermitian operator $A \in B(\mathcal{H})$ such that*

$$\mathrm{Tr}\,(A\rho) < 0 \quad and \quad \mathrm{Tr}\,(A\sigma) \geq 0$$

for all $\sigma \in C$.

This theorem is an immediate consequence of basic theorems in functional analysis [181, 247]. Namely, the Hahn-Banach theorem states that a convex set and a point lying outside it can be separated by a hyperplane W, and the Riesz-Frechet representation theorem then characterizes such hyperplanes. The hyperplanes W are commonly called witnesses [284] (they witness states outside C).

Corollary 1.2.1 (Horodecki et al. [132])**.** *A state $\rho \in \mathcal{D}$ is separable if and only if* $\mathrm{Tr}(\rho W) \geq 0$ *for all Hermitian operators W such that* $\mathrm{Tr}([|\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|]W) \geq 0$, *with $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$. Such operators W will be referred to as entanglement witnesses.*

---

[1]R. Werner, LMS Workshop on quantum information and computation (York 2005).

We have encountered an entanglement witness when we discussed the CHSH in-equality. From our discussion, it is easy to see that

$$W_{\text{CHSH}} = 2\mathbb{1} - [\vec{a} \cdot \vec{\sigma} \otimes (\vec{b} + \vec{b'}) \cdot \vec{\sigma} + \vec{a'} \cdot \vec{\sigma} \otimes (\vec{b} - \vec{b'}) \cdot \vec{\sigma}], \qquad (1.2)$$

is an entanglement witness. Here $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is a vector containing the Pauli spin matrices [161, 163, 284]. Note also that a general entanglement witness W can be measured locally, by decomposing it as (non-convex) sum of product states. The problem of finding an optimized decomposition both in the optimal number of projectors on product vectors and in the optimal number of settings of the detectors has been partially solved in Ref. [107, 108].

Let us now give two examples of entanglement witnesses, which will be important for the sequel. The first one [132] is the so-called swap or flip operator F, which acts on state vectors as $F|\psi_A\rangle|\psi_B\rangle = |\psi_B\rangle|\psi_A\rangle$ or in a basis $\{|ij\rangle\}$ of $\mathcal{H}$:

$$F = \sum_{ij} |ij\rangle\langle ji|.$$

It is not so hard to check that this operator is indeed positive on product states. The swap operator is an entanglement witness because F has negative eigenvalues and will therefore necessarily act negative on some state (for instance for $|\psi_-\rangle$). The second example is given by

$$W_{\text{R}} = \mathbb{1} - dP_+$$

with P_+ the projector onto the maximally entangled state $|\psi_+\rangle = \frac{1}{\sqrt{d}} \sum_i |ii\rangle$. Since the maximum overlap of a separable state with P_+ is $1/d$, and since W has negative eigenvalues, it is an entanglement witness (for instance for $|\psi_+\rangle$).

Intuitively the value $\min_W \text{Tr}(\rho W)$ can be associated with the distance of ρ to the set of separable states and in some way is related to the degree of entanglement of ρ. However, as such the minimum is ill-defined as the set of entanglement witnesses is unbounded. This can be overcome by imposing suitable constraints on the entanglement witnesses W, and it turns out that in this way a variety of geometrical intuitive entanglement measures can be obtained [33, 230]. We will come back to the topic of geometrical entanglement measures briefly in Chapter 2.

1.2.2   Jamiołkowski isomorphism and positive maps

In this section we will reformulate the characterisation of separable states (Corollary 1.2.1) in terms of positive maps. This can be done by making use of the Jamiołkowski isomorphism which establishes a one-to-one correspondence between linear operators and linear maps between operator spaces. We will outline the isomorphism and illustrate it for Hermitian preserving, positive and completely positive maps. We then apply it to the examples of last section, and obtain the reduction and the partial transpose criteria, respectively. The results outlined in this section date back to the 1970-80s' [53] but have only recently [132] been used in quantum information. This section is meant as an introduction to the isomorphism and we will see more about positive maps and the context in which they were studied in Section 1.2.3.

A Hermitian map $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ is a *linear* map that maps Hermitian operators onto Hermitian operators. A positive map $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ is a linear map that maps positive operators $\rho \geq 0$ onto positive operators $\Lambda(\rho) \geq 0$. A k-positive map is a positive map such that the induced map

$$\Lambda_k = \mathbb{1}_k \otimes \Lambda : \mathcal{L}_{\mathbb{C}^k} \otimes \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathbb{C}^k} \otimes \mathcal{L}_{\mathcal{H}_B}$$

is positive for $k \geq 1$. A complete positive map (CP map) is a k-positive map for all positive k.

In the proof of the Schmidt decomposition we found it useful to interpret the coefficients ψ_{ij} in the expansion of $|\psi\rangle = \sum_{ij} \psi_{ij}|ij\rangle$ as the matrix $\{\psi_{ij}\}$ of an operator Ψ. With this notation one can equally write

$$|\psi\rangle = \sqrt{d}(\Psi \otimes \mathbb{1})|\psi_+\rangle = \sqrt{d}(\mathbb{1} \otimes \Psi^T)|\psi_+\rangle. \tag{1.3}$$

This relation in effect establishes an explicit isomorphism between $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ [25] and comes back frequently in quantum information (see for example [295, 296, 340]). Suppose now that we have a general Hermitian operator $W \in \mathcal{L}_{\mathcal{H}_A \otimes \mathcal{H}_B}$, using the spectral decomposition we can write

$$W = \sum_i w_i |\phi_i\rangle\langle\phi_i|,$$

with all coefficients w_i real. Using the above isomorphism we associate with every

vector $|\phi_i\rangle$ the matrix Φ_i and write

$$W = d \sum_i w_i (\mathbb{1} \otimes \Phi_i) P_+ (\mathbb{1} \otimes \Phi_i^\dagger).$$

Defining a map Λ_W as acting as

$$\Lambda_W(A) = \sum_i w_i \Phi_i A \Phi_i^\dagger, \tag{1.4}$$

for all A, this can be written as

$$W = d(\mathbb{1} \otimes \Lambda_W) P_+. \tag{1.5}$$

It is clear that when a linear map Λ_W can be written in the form of (1.4) it is automatically a Hermitian map. Conversely, using the above correspondence (1.5), it is easy to see that any Hermitian map Λ_W will correspond to a Hermitian operator W and therefore can be written in the form (1.4). When W is a positive operator, all the coefficients w_i will be positive and Λ_W will become a completely positive operator. Conversely, it is again easy to see that any completely positive map can be written in the form (1.4). These results were first derived by de Pillis [67] and Choi [49] respectively (see also Ref. [124, 131, 174, 178, 232, 276, 296]), we summarise them in the following theorem.

Theorem 1.2.3. *A linear map $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ is Hermitian (completely positive) if and only if for all operators $A \in \mathcal{L}_{\mathcal{H}_A}$ it can be written as*

$$\Lambda(A) = \sum_i \lambda_i V_i A V_i^\dagger,$$

for some operators $V_i : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$, and real (positive) numbers λ_i.

In the proof of this theorem we made use of the relation $W = d(\mathbb{1} \otimes \Lambda_W) P_+$ which associates with each linear map Λ_W an operator W. Note that W defines uniquely the map Λ_W since a linear map is determined by its action on the basis $\{|i\rangle\langle j|\}$. Indeed, it is not so hard to see that (1.5) can be written as

$$\langle k|\Lambda_W(|i\rangle\langle j|)|l\rangle = \langle ik|W|jl\rangle. \tag{1.6}$$

Thus in this way we have defined an isomorphism between linear maps $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ and operators $W \in \mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B}$. This is the famous Jamiołkowski isomorphism and can also be written as

$$\Lambda_W(X) = \mathrm{Tr}_A[W(X^T \otimes \mathbb{1})].$$

Linear maps Λ $\longleftrightarrow$ $\mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B}$ $\longleftrightarrow$ Linear functionals on

$(\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B})$ $\mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B}$

Hermitian maps $\longleftrightarrow$ $(\mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B})^h$ $\longleftrightarrow$ Linear functionals

assuming real values

on $(\mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B})^h$

Positive maps $\longleftrightarrow$? $\longleftrightarrow$ Linear functionals

acting positive

on $\mathcal{L}_{\mathcal{H}_A}^+ \otimes \mathcal{L}_{\mathcal{H}_B}^+ (\text{or } S)$

k-Positive maps $\longleftrightarrow$? $\longleftrightarrow$ Linear functionals

assuming positive

values on S_k

CP maps $\longleftrightarrow$ $(\mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B})^+$ $\longleftrightarrow$ Linear functionals

acting positive

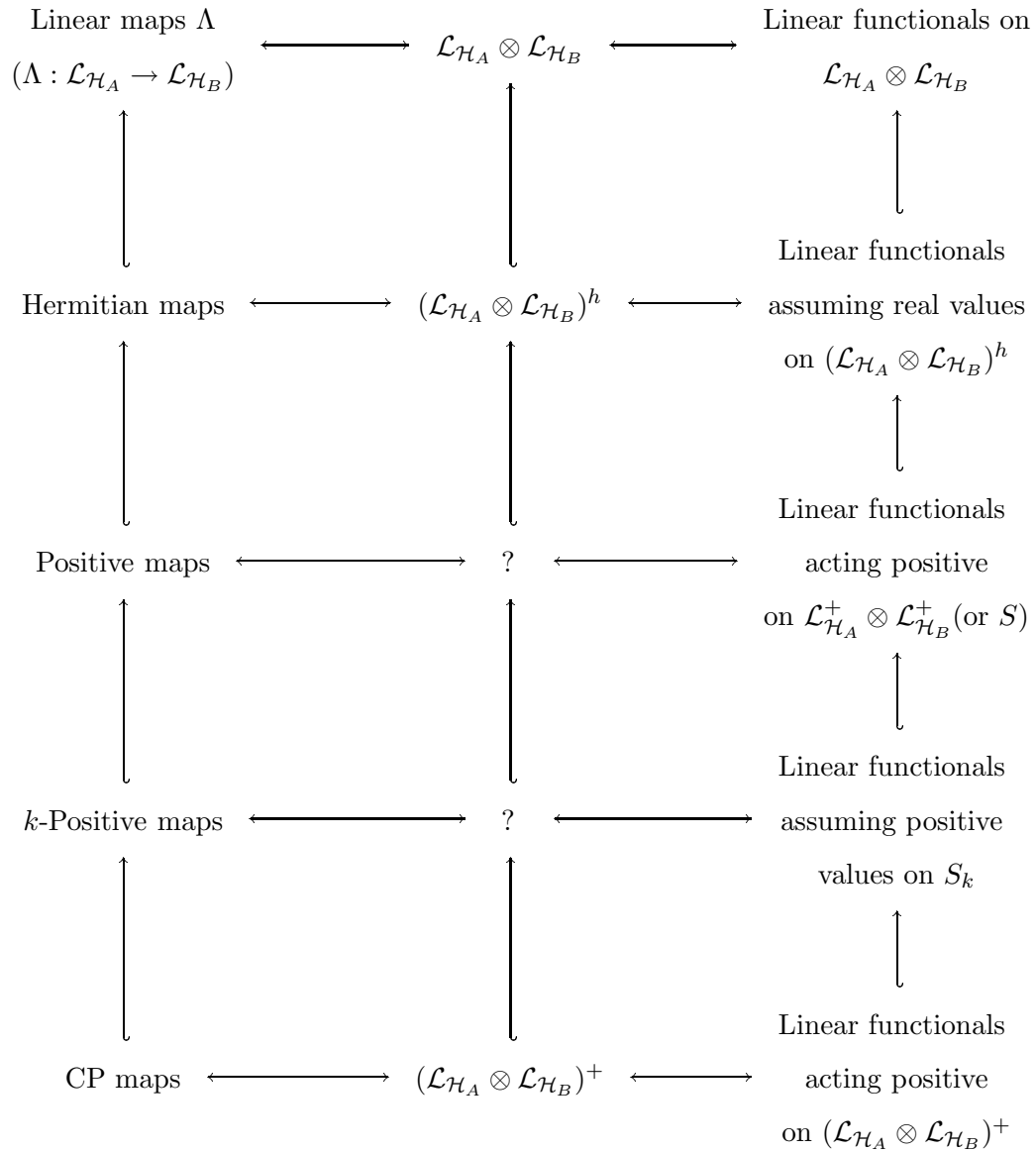on $(\mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B})^+$

Figure 1.1: The Jamiołkowski isomorphism and correspondences for important classes of linear maps. The correspondence for k-positive maps will be outlined in Chapter 2. Except for the addition of these maps this chart is from Ref. [53].

Jamiołkowski [166] derived this isomorphism in order to characterise positive maps. As a positive map is Hermitian we can always write it in the form of (1.4). However it is unclear how to distinguish between Hermitian and positive maps from this. The trick is to associate with the operator W the linear functional $f_W(|\psi\rangle) = \langle\psi|W|\psi\rangle$, this linear functional can be characterised as follows.

Theorem 1.2.4. *A linear map* $\Lambda_W : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ *is positive if and only if the corresponding functional* f_W *on* $\mathcal{H}_A \otimes \mathcal{H}_B$ *is positive on product vectors.*

Proof. We can prove this theorem solely by examining (1.6) for the special case where $|i\rangle = |j\rangle = |x\rangle$ and $|k\rangle = |l\rangle = |y\rangle$:

$$\langle y|\Lambda_W(|x\rangle\langle x|)|y\rangle = \langle xy|W|xy\rangle.$$

If f_W is positive on product vectors then Λ_W is positive on projectors, and therefore on arbitrary positive operators also. If Λ_W is a positive map, then from the above equation follows that f_W is positive on product vectors. $\qquad\square$

Thus in the language of the previous section, positive maps correspond to entanglement witnesses. Figure 1.1 summarises the isomorphism and its relations for different classes of linear maps. With this we are in the position of stating the main result of this section, which was first published in Ref. [132] (note that it can be extended to multipartite systems, for details see Ref. [139]).

Theorem 1.2.5. *A density operator* ρ *acting on* $\mathcal{H}_A \otimes \mathcal{H}_B$ *is separable if and only if*

$$(\mathbb{1} \otimes \Lambda)(\rho) \geq 0,$$

for all positive maps $\Lambda : \mathcal{L}_{\mathcal{H}_B} \to \mathcal{L}_{\mathcal{H}_A}.$

Proof. With each linear map $\Lambda : \mathcal{L}_{\mathcal{H}_B} \to \mathcal{L}_{\mathcal{H}_A}$ there is associated an adjoint map $\Lambda^\dagger : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ defined by

$$\mathrm{Tr}[A\Lambda(B)] = \mathrm{Tr}[\Lambda^\dagger(A)B]$$

for all operators A, B. It is easy to verify that the adjoint map of a positive map is again positive. Suppose now that ρ is entangled, then from Corollary 1.2.1 follows

that there exists an entanglement witness W such that $\text{Tr}(\rho W) < 0$. By virtue of the Jamiołkowski isomorphism and Theorem 1.2.4 this is equivalent to

$$\text{Tr}[(\mathbb{1} \otimes \Lambda_W)(P_+)\rho] = \text{Tr}[(\mathbb{1} \otimes \Lambda_W^\dagger)(\rho)P_+] < 0$$

and since P_+ is positive it follows that $(\mathbb{1} \otimes \Lambda_W^\dagger)(\rho) \not\geq 0$. Conversely, let $\Lambda_W^\dagger$ be a positive map such that $(\mathbb{1} \otimes \Lambda_W^\dagger)(\rho)$ has a negative eigenvalue with corresponding eigenvector $|\phi\rangle = A \otimes \mathbb{1}|\psi_+\rangle$. With this we get

$$\langle\phi|\mathbb{1} \otimes \Lambda_W^\dagger(\rho)|\phi\rangle = \text{Tr}[(A \otimes \mathbb{1})W(A^\dagger \otimes \mathbb{1})\rho] < 0.$$

Since W is positive on separable states, the same applies to $(A \otimes \mathbb{1})W(A^\dagger \otimes \mathbb{1})$. This shows that ρ must be entangled. $\qquad\square$

The proof of Theorem 1.2.5 reveals two important facts about the relation between entanglement witnesses and positive maps. Namely, given an entanglement witness W, the corresponding positive map $\Lambda_W^\dagger$ will always detect more states than the witness, as it detects all states detected by the class of witnesses $(A \otimes \mathbb{1})W(A^\dagger \otimes \mathbb{1})$ for all operators A. Furthermore, if a certain positive map Λ_W is negative on a state ρ, then the proof shows us how to construct an operator A such that the local transformation[2]

$$\rho \longrightarrow (A^\dagger \otimes \mathbb{1})\rho(A \otimes \mathbb{1}), \tag{1.7}$$

will yield a state that can be detected by the entanglement witness W.

In the previous section, we have seen two important examples of entanglement witnesses. The map associated with $W = \mathbb{1} - dP_+$ is given by $\Lambda(A) = \mathbb{1}\,\text{Tr}(A) - A$. From this follows that all separable states ρ satisfy

$$\rho_A \otimes \mathbb{1} - \rho \geq 0 \qquad \text{and} \qquad \mathbb{1} \otimes \rho_B - \rho \geq 0,$$

while this is not necessarily the case for entangled states. It is not so hard to prove the positivity of this map directly. The associated separability criterion is called the reduction criterion and was first studied in Ref. [43, 131].

Another entanglement witness was given by the swap operator F. It is not so hard to see that the associated map is given by the transposition. For a separable state

---

[2]See Section 3.1 for more on quantum operations.

$\rho = \sum_i p_i |\psi_i^A\rangle\langle\psi_i^A| \otimes |\psi_i^B\rangle\langle\psi_i^B|$ we have that $(\mathbb{1} \otimes T)\rho \geq 0$, while this is not necessarily the case for entangled states. We write $(\mathbb{1} \otimes T)\rho = \rho^{T_B}$ and call this operation the partial transposition. When $\rho^{T_B} \geq 0$ we say that the state has a positive partial transpose (PPT), otherwise the state has a negative partial transpose (NPT). The partial transposition criterion was first discovered by Peres [223] independently of the notion of positive maps. This criterion turns out to be powerful, in particular, positivity of the partial transposition is necessary and sufficient for separability when $\dim \mathcal{H} \leq 6$ [132]. It was subsequently shown also to be necessary and sufficient for states with low rank [151], in particular for pure states [284], rank two states [153] and rank three states [151]. In general though, it is not sufficient, and there exist PPT entangled states. We will see an example of such a PPT entangled state in the next section, where we also analyse the importance of the partial transposition in the structure of positive maps. We will denote the set of PPT states as $\mathcal{P}$. The set $\mathcal{P}$ is, just like the set of separable states $\mathcal{S}$, compact and $\mathcal{S} \subset \mathcal{P} \subset \mathcal{D}$.

It can be shown that the reduction criterion is strictly weaker than the partial transposition criterion [131], except when $\dim \mathcal{H}_B = 2$ or $\dim \mathcal{H}_A = 2$ in which case both criteria are equivalent. This last statement follows from the identity $\mathbb{1} \operatorname{Tr}(A) - A = (\sigma_y A \sigma_y)^T$ for two dimensional matrices A. The reduction and the partial transposition criterion are important in the context of distillation, they will be studied in detail in Chapter 3.

1.2.3   Some deeper results

We start this section with the following classical theorem, which gives a complete characterisation of positive maps between low dimensional operators (for elementary proofs see Ref. [84, 183, 298]):

Theorem 1.2.6 (Størmer and Woronowicz [277, 328])**.** *Let $\Lambda : \mathcal{L}_{\mathbb{C}^2} \to \mathcal{L}_{\mathbb{C}^n}$ be a positive map, with $n \leq 3$. Then Λ can be written as*

$$\Lambda = \Lambda_1 + \Lambda_2 \circ T,$$

with Λ_1, Λ_2 completely positive maps.

We call a positive map decomposable if it can be written as a combination of a completely positive map and the combination of a completely positive map and transposition. It is easy to see that entangled states detected by a decomposable map will also be detected by the partial transposition alone. Thus from Theorem 1.2.5 we obtain that for all bipartite states ρ acting on $\mathcal{H}$ with $\dim \mathcal{H} \leq 6$, positivity of the partial transposition is a necessary and sufficient condition for separability.

The first example of an undecomposable map was given by Choi [50, 51, 52]. Let $\Lambda_C : \mathcal{L}_{\mathbb{C}^3} \to \mathcal{L}_{\mathbb{C}^3}$ be the linear map defined as

$$\Lambda_C(A) = \begin{bmatrix} A_{11} + A_{33} & -A_{12} & -A_{13} \\ -A_{21} & A_{22} + A_{11} & -A_{23} \\ -A_{31} & -A_{32} & A_{33} + A_{22} \end{bmatrix}, \tag{1.8}$$

for all 3×3 matrices $A = [A_{ij}]$. He originally proved that this map is positive on real positive semidefinite (and thus symmetric) matrices , but it easy to see that this implies that the map is positive on all positive semidefinite matrices [52]. With a counterexample, we will show that this map is not decomposable. The example is due to Størmer [278] but analysed in the context of entanglement in Ref. [75, 138, 149]. Define for $0 \leq \alpha \leq 5$

$$\sigma = \frac{1}{7} \left[2P_+ + \alpha \sigma_+ + (5 - \alpha)\sigma_- \right], \tag{1.9}$$

with

$$\sigma_+ = \frac{1}{3}(|01\rangle\langle 01| + |12\rangle\langle 12| + |20\rangle\langle 20|)$$

and $\sigma_- = F\sigma_+ F$. This state has a positive partial transpose for $1 \leq \alpha \leq 4$, for other α the state is NPT entangled. Now it is easy to verify that $(\mathbb{1} \otimes \Lambda_C)(\sigma)$ is not positive for $3 \leq \alpha \leq 4$ and $1 \leq \alpha \leq 2$ since it has an eigenvalue $\lambda = (3 - \alpha)/2$. This immediately shows that Λ_C is non-decomposable and that σ is PPT entangled in these regions. For the region $2 \leq \alpha \leq 3$, the state can be shown to be separable by virtue of an explicit decomposition in terms of product states. Following Choi's example, many other non-decomposable maps have been found and studied in the literature, see for instance Ref. [56, 111, 115, 179, 187, 200, 217, 246, 281, 282, 289, 328].

The notion of decomposability can also be extended to entanglement witnesses via the Jamiołkowski isomorphism. Namely it is easy to see that any decomposable map

Λ_W corresponds to a witness

$$W = P + Q^{T_B},$$

with P and Q positive semidefinite (and vice verse). We will refer to such witnesses as decomposable witnesses. There exists [185, 186] a canonical representation of inde-composable entanglement witnesses, which we will derive now. Central is the idea of a so-called edge state, which is a PPT entangled state δ such that for all $\epsilon \geq 0$ and all separable $|ab\rangle$,

$$\delta - \epsilon|ab\rangle\langle ab|$$

is not positive or does not have a positive partial transpose. Edge states can be thought of as lying on the boundary between PPT and NPT states, and thus in this sense, they are the most entangled PPT states. From the definition it is clear that a state δ is an edge state if and only if there is no product vector $|ab\rangle$ in the range of δ such that $|ab^*\rangle$ is in the range of δ^{T_B}. If such a product vector exists, we could subtract it from the state and still obtain a PPT state. Repeating this process will eventually yield an edge state (see also Figure 1.2):

Theorem 1.2.7. *Every PPTES ρ can be decomposed as*

$$\rho = (1 - p)\rho_{sep} + p\delta,$$

with ρ_{sep} a separable state and δ an edge state.

The following theorem provides a canonical construction of an entanglement wit-ness that detects a given edge state. Conversely it states that any non-decomposable entanglement witness can be written in a similar form.

Theorem 1.2.8. *(i) Let δ be an edge state with P and Q the projector onto the kernel of δ and δ^{T_B} respectively. Let*

$$W_\delta = P + Q^{T_B},$$

and

$$\epsilon = \inf_{|ab\rangle} \langle ab|W_\delta|ab\rangle,$$

then $W_1 = W_\delta - \epsilon \mathbb{1}$ is an non-decomposable entanglement witness which detects δ.

Figure 1.2: Schematic representation of the nesting $\mathcal{S} \subset \mathcal{P} \subset \mathcal{D}$ and a PPT state as the convex combination of an edge and a separable state [39].

(ii) Any non-decomposable witness W can be written as

$$W = P + Q^{T_B} - \epsilon \mathbb{1}$$

with

$$0 < \epsilon \leq \inf_{|ab\rangle} \langle ab| P + Q^{T_B} |ab\rangle.$$

Here P, Q are positive semidefinite and satisfy $\operatorname{Tr} P\delta = \operatorname{Tr} Q^{T_B}\delta = 0$ for some edge state δ.

Proof. (i) As the range of δ contains no product vector $|ab\rangle$ such that the range of δ^{T_B} contains $|ab^*\rangle$, there must exist such a product vector in their respective kernels, so that $\epsilon > 0$. By its very definition, W_1 is positive on product states and since $\operatorname{Tr}(W_1\delta) = -\epsilon < 0$ it is an non-decomposable entanglement witness which detects δ.

(ii) Let $W(\lambda) = W + \lambda\mathbb{1}$ with $\lambda > 0$. We denote with λ_0 the smallest λ such that $W(\lambda_0) = 0$ is decomposable. Since $W(\lambda_0)$ is decomposable we can write it as $W(\lambda_0) = P + Q^{T_B}$ and thus $W = P + Q^{T_B} - \lambda_0\mathbb{1}$. Using the compactness of the set of PPT states $\mathcal{P}$ there will exist a state ρ such that $\operatorname{Tr}(\rho W(\lambda_0)) = 0$. Now let $\rho = (1-p)\rho_{\text{sep}} + p\delta$, with δ an edge state, so that

$$p \operatorname{Tr}(W\rho_{\text{sep}}) + (1-p) \operatorname{Tr}(W\delta) = -\lambda_0.$$

When $p > 0$ this would lead to $\mathrm{Tr}(W(\lambda_0)\delta) < 0$, contrary to the assumption that $W(\lambda_0)$ is decomposable. So $p = 0$, $\mathrm{Tr}(\delta W(\lambda_0)) = 0$ and $\mathrm{Tr}(\delta W) = -\lambda_0$. It follows that $\mathrm{Tr}\,P\delta = \mathrm{Tr}\,Q^{T_B}\delta = 0$. The theorem follows by putting $\epsilon = \lambda_0$, where the condition on ϵ follows because W is an entanglement witness. $\qquad\square$

This theorem can be generalised straightforwardly to arbitrary convex sets and associated witnesses [39]. In Ref. [185, 186] it was shown how to optimise a non-decomposable witness W (for instance constructed from an edge state). Optimising in this context means iterative subtraction of decomposable witnesses from W, yielding a stronger witness. We refer to the original references for details.

With an entanglement witness W or alternatively the positive map Λ_W we can associate the following bihermitian positive form:

$$F_W(x_i, y_i) = \langle xy|W|xy\rangle = \langle x|\Lambda_W(|y\rangle\langle y|)|x\rangle = \sum_{ijkl} W_{ij;kl} x_i^* y_j^* x_k y_l.$$

Suppose now that Λ_W has real coefficients in some basis, then for real x_i, y_i, F_W is a so-called real biquadratic form. Hilbert's 17th Problem is concerned with the question whether all real positive semidefinite forms can be written as the sum of squares (SOS) of forms (see Ref. [245] for an excellent overview on Hilbert's 17th problem). Choi [50, 52, 53, 284] showed that non-decomposable maps with real coefficients allow to construct counterexamples for biquadratic forms.

Theorem 1.2.9. *(i) Let F_W be a real biquadratic form which cannot be written as a SOS of linear forms, then the associated map Λ_W is non-decomposable. (ii) Conversely, if Λ_W is a non-decomposable with real coefficients, then F_W cannot be expressed as a SOS.*

Proof. (i) Note that decomposable maps acting on (real) symmetric matrices act as completely positive maps, so we can write

$$\Lambda_W(|y\rangle\langle y|) = \sum_l A_l|y\rangle\langle y|A_l^T,$$

and with $\langle x|A_l|y\rangle = a_{ij}^l$ we get

$$F_W(x_i, y_i) = \langle x|\Lambda_W(|y\rangle\langle y|)|x\rangle = \sum_l \langle x|A_l|y\rangle\langle y|A_l^T|x\rangle = \sum_l (a_{ij}^l x_i y_j)^2.$$

(ii) By reversing the argument of (i) it follows that if F_W can be expressed as a SOS, then Λ_W is decomposable. □

Earlier in this section we have seen Choi's example of an non-decomposable map. The associated real form is given by

$$F_C = x_1^2 y_1^2 + x_2^2 y_2^2 + x_3^2 y_2^2 - 2(x_1 x_2 y_1 y_2 + x_2 x_3 y_2 y_3 + x_3 x_1 y_3 y_1) + x_1^2 y_2^2 + x_2^2 y_3^2 + x_3^2 y_1^2.$$

By inspection Choi showed the positivity of this form and showed that it cannot be expressed as a SOS. This immediately proves the non-decomposability of the associated map.

For a more abstract formulation of the separability problem, with various connections to C^*-algebras the reader is referred to the series of papers by Majewski et al. [196, 197, 198, 199].

1.2.4   PPT entangled states

In this section we provide several ways of constructing PPT entangled states, with particular emphasis on the UPB construction and the range criterion. Based on this, we construct two new entangled PPT states with special ranks. For completeness, references will be listed to all other PPT entangled states known to us.

In the previous section we have seen Størmer's example [75, 149, 278] of a PPT state, constructed such that it is detected by Choi's indecomposable map. In general given an indecomposable map, one can try to guess from it some state which is PPT entangled [138], see for example the PPT states constructed in Ref. [18, 36, 226]. Recently, it has been shown how to systematically construct PPT entangled states from a given indecomposable map [112, 113, 114]. Yet despite this advance, coming up with an indecomposable map is highly non-trivial and very much a matter of trial and error.

Currently, the only systematic way of constructing PPT entangled states is based on unextendible product basis (UPB) [23, 73]. An UPB in a Hilbert space $\mathcal{H} = \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ is a set of pure orthogonal product states which do not span[3] $\mathcal{H}$ and such that there is no product vector orthogonal to all of them. This definition is readily extended

---

[3]Therefore, an unextendible product basis is in fact not a basis.

to multipartite systems. As an example, consider the following set of vectors S in $\mathcal{H} \cong \mathbb{C}^3 \otimes \mathbb{C}^3$:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle), \qquad |\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle,$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle), \qquad |\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle,$$

$$|\psi_4\rangle = \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle).$$

Now if this set of vectors is extendible, then there has to exist a partition of this set of vectors S, into two subsets S_1 and S_2, such that the local rank of the first subsystem for S_1 is smaller than 3, and the local rank of the second subsystem for S_2 is smaller than 3. In this case, one can construct a vector $|ab\rangle$ such that $|a\rangle$ is orthogonal to the first subsystem of S_1 and $|b\rangle$ is orthogonal to the second subsystem of S_2. But this is impossible since either S_1 or S_2 will contain at least three vectors, and it is easy to see that any three vectors, seen by either party span the full space of that party. We refer to the original papers and the review [71] for a plethora of other examples.

From any UPB one can construct a bound entangled state as in the next theorem.

Theorem 1.2.10. *Let the set of n vectors $\{|\psi_i\rangle\}$ be a UPB in $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$, with* $\dim \mathcal{H} = d$, *then*

$$\rho = \frac{1}{d-n}(\mathbb{1} - \sum_{j=1}^n |\psi_j\rangle\langle\psi_j|)$$

is a PPT entangled state.

Proof. The state ρ has positive partial transposition as the set $\{|\psi_j\rangle\langle\psi_j|^{T_B}\}$ is again a UPB. It is easy to see that ρ is entangled and in fact an edge state as, by definition, there is no product state in the space orthogonal to the UPB. $\square$

In Ref. [285] it was shown how to systematically construct entanglement witnesses detecting UPB states. The generalisation of this construction for general edge states is precisely the one we outlined in the previous section (Theorem 1.2.8). Based on these witnesses, PPT entangled states in the neighbourhood of UPB PPT entangled states can be constructed [15, 228].

As we have seen, an edge state ρ contains no product vector $|a_i b_i\rangle$ in its range such that $|a_i b_i^*\rangle$ is in the range of ρ^{T_B}. This condition is clearly a sufficient for a state to be PPT entangled. We can make this criterion slightly stronger as follows [146]:

Theorem 1.2.11 (Range criterion)**.** *If a state ρ is separable there must exist a set of product vectors $\{|a_i b_i\rangle\}$ spanning the range of ρ such that $\{|a_i b_i^*\rangle\}$ span the range of ρ_B^T.*

Thus edge states violate the range criterion in the strongest way. The range criterion was originally devised by Woronowicz [328] in the context of indecomposable maps. This criterion is remarkable simple and powerful, in particular for proving the PPT property of sparse matrices. Examples of states violating the range criterion have been published in Ref. [38, 53, 97, 146, 148, 328]. Various other PPT entangled states have appeared over the years [1, 11, 75, 79, 128, 129, 152, 165, 227, 310, 322, 332]. In most cases the states are shown to be inseparable by showing that they can help performing some non-classical tasks. In Section 4.4 we will say more about these so-called activation processes.

We conclude this section with the presentation of two new PPT states [62]. The new types are $(5,5)$ and $(6,6)$ edge states. Here in (N, M), N denotes the rank of the state, while M denotes the rank of ρ^{T_B}. The question of their existence popped up in the analysis of a conjecture on 2-positive maps between 3×3 matrices. We come back to this conjecture in Section 2.3.

A $(5,5)$ edge PPTES

Consider the following $(5,5)$ state:

$$\rho_{(5,5)} = \frac{1}{13} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 3 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & -2 & 3 \end{bmatrix},$$

and its partial transpose:

$$
\rho_{(5,5)}^{T_B} = \frac{1}{13}
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 1 & 0 & 0 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 3 & 0 & -1 & -1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & -2 \\
0 & 0 & -1 & 1 & 0 & 0 & 0 & -2 & 3
\end{bmatrix}.
$$

It is not so hard to verify that both operators are positive semi-definite and have rank 5. An analytical expression of their eigenvectors and eigenvalues is however quite complex. To show that $\rho_{(5,5)}$ is an edge state we will show that it violates strongly the range criterion. For this we will use the 'divide and conquer technique' from [146].

From the matrix representation above we see that every vector in the range of $\rho_{(5,5)}$ can be written in the form

$$
V = (0, A, -E - F, C, 0, D, D, E, F), \quad A, C, D, E, F \in \mathbb{C}.
$$

Now we have look at those vectors which can be written as a product

$$
V = (s, t, v) \otimes (x, y, z) = (sx, sy, sz, tx, ty, tz, vx, vy, vz).
$$

Taking these two conditions together we can therefore characterise all product vectors in the range of $\rho_{(5,5)}$.

From the condition $sx = 0$ we can distinguish the following sub cases:

1. $x = 0, s \neq 0$, we have $vx = D = 0 = tz$ and therefore either $t = 0$ or $z = 0$. Without loss of generality we can also put $s = 1$.

1.1. $t = 0$, as $v(y + z) = -z$ we have $v = -z/(y + z)$. When $y = -z$, then $z = 0 = -y = x$ and we obtain the null vector. Thus the only case that remains is

$$
V = s \left(1, 0, \frac{-z}{y + z} \right) \otimes (0, y, z),
$$

with $y \neq -z$.

1.2. $z = 0$, from $ty = 0$ follows that $t = 0$ (otherwise $y = 0$) thus this case is already covered in 1.1.

2. $s = 0$, from $E = -F$ follows that $vy = -vz$. From $ty = 0$ follows that either $t = 0$ or $y = 0$.

2.1 $t = 0$, since $D = 0 = vx$ we have that $x = 0$ and $v \neq 0$, and thus $z = -y$. Thus we get

$$V = (0, 0, v) \otimes (0, y, -y)$$

2.2 $y = 0$, and thus $vy = -vz = 0$ so either $z = 0$ or $v = 0$.

2.2.1 $z = 0$, and thus $vx = tz = 0$. Because $x \neq 0$ we have that $v = 0$:

$$V = (0, t, 0) \otimes (x, 0, 0)$$

2.2.2 $v = 0$ and thus $vx = tz = 0$. Because $t \neq 0$ we have that $z = 0$ and we arrive at 2.2.1.

We now do the same analysis for $\rho_{(5,5)}^{T_B}$. It is easy to see that every vector in its range can be written as

$$V = (0, A, B, C, 0, D, E, A + 2B, -A - 2B + C + D + E),$$

with $A, B, C, D, E \in \mathbb{C}$. We need to take the intersection of these vectors with those vectors which can be written as a product

$$V = (s, t, v) \otimes (x, y, z) = (sx, sy, sz, tx, ty, tz, vx, vy, vz).$$

From the condition $sx = 0$ we can distinguish the following sub cases:

1. $x = 0$, and since $ty = 0$ we have that $y = 0$ or $t = 0$

1.1. $y = 0$ and thus $vy = 0$ and $sy = -2sz = 0$. Since $z = 0$ gives the null vector we get $s = 0$. Now $vz = -sy - 2sz + tx + tz + vx = tz$ and thus $t = v$, and thus

$$V = (0, t, t) \otimes (0, 0, z)$$

1.2. $t = 0$, and since $vz = -sy - 2sz = -vy$ either $v = 0$ or $z = -y$

1.2.1. $v = 0$ and thus $sy = -2sz$ or since $s = 0$ is trivial we get $y = -2z$ and thus

$$V = (s, 0, 0) \otimes (0, -2z, z)$$

1.2.2. $z = -y$, and thus $-vy = -sy + 2sy = sy$. Since $y = -z = 0$ is trivial we get $v = -s$ and

$$V = (-s, 0, s) \otimes (0, y, -y)$$

2. $s = 0$ and thus $vy = 0$, we also have $ty = 0$ thus either $y = 0$ or $v = t = 0$, but this last case gives us again the trivial vector. From $vz = -sy - 2sz + tx + ty + tz + vx = tx + tz + vx$ we have $(v - t)z = (v + t)x$. What remains is

$$V = (0, v, t) \otimes (x, 0, z),$$

with either $z = \frac{v+t}{v-t}x$ or $x = \frac{v-t}{v+t}z$ (but only one of those when $v = \pm t$).

It is now straightforward to check that when $v = (s, t, v) \otimes (x, y, z)$ belongs to the range of $\rho_{(5,5)}$ that $v' = (s, t, v) \otimes (x^*, y^*, z^*)$ does not belong to the range of $\rho_{(5,5)}^{T_B}$. This concludes the proof that $\rho_{(5,5)}$ is a $(5, 5)$ edge state.

A $(6, 6)$ edge PPTES

Consider the following state

$$\rho_{(6,6)} = \frac{1}{13} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 \end{bmatrix},$$

with partial transpose

$$\rho_{(6,6)}^{T_B} = \frac{1}{13} \begin{bmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 3 \end{bmatrix}.$$

It can be checked easily that both matrices are positive definite and have rank 6. Following a similar strategy as in the previous section we now proceed to show that $\rho_{(6,6)}$ is an edge state. Every vector in the range of $\rho_{(6,6)}$ can be written in the form

$$V = (A, B, C, D, E, F, C + E, -F, B + 2D - A), \tag{1.10}$$

with $A, B, C, D, E, F \in \mathbb{C}$, whilst every vector in the range of $\rho_{(6,6)}^{T_B}$ takes the form

$$V' = (A, B, C, D, -A, E, E - C, D, F), \tag{1.11}$$

with $A, B, C, D, E, F \in \mathbb{C}$. The 'divide and conquer' method does not work so well here as we have no zeros to start with. Instead we will show directly that if the product vector

$$V = (s, t, v) \otimes (x, y, z) = (sx, sy, sz, tx, ty, tz, vx, vy, vz).$$

belongs to the range of $\rho_{(6,6)}$, then $V' = (s, t, v) \otimes (x^*, y^*, z^*)$ does not belong to the range of $\rho_{(6,6)}^{T_B}$. Comparing equations (1.10) and (1.11) with their product form we get the following set of equations:

$$vx = sz + ty$$

$$vy = -tz$$

$$vz = sy + 2tx - sx$$

$$ty^* = -sx^*$$

$$vx^* = tz^* - sz^*$$

$$vy^* = tx^*$$

We consider the following sub case

1. $vy \neq 0$, and it follows that all parameters are different from zero. Without loss of generality we can put $x = 1$ and get

$$v = sz + ty$$
$$vy = -tz$$
$$vz = sy + 2t - s$$
$$ty^* = -s$$
$$v = tz^* - sz^*$$
$$vy^* = t$$

We now use $t = vy^*$ and $s = -v(y^*)^2$ to eliminate t and s, after which we can divide every equation by v resulting in

$$1 = -(y^*)^2 z + y^* y$$
$$y = -y^* z$$
$$z = -(y^*)^2 y + 2y^* + (y^*)^2$$
$$1 = y^* z^* + (y^*)^2 z^*$$

From the first and the second equation we get $yy^* = \frac{1}{2}$, while from the second and fourth equation we get $1 = y^*(z^* - y)$ or $y = yy^*(z^* - y) = \frac{1}{2}(z^* - y)$ and thus $z = 3y^*$. From the third equation we get

$$3y^* = -(y^*)^2 y + 2y^* + (y^*)^2$$

or

$$3 = -y^* y + 2 + y^*$$

and thus $y^* = \frac{3}{2}$ which contradicts $yy^* = \frac{1}{2}$.

2. $v = y = 0$, in this case it is straightforward to see that $x = y = z = 0$.

3. $y = 0$ and $v \neq 0$. From $sx^* = 0$ and $tx^* = 0$ follows that $s = t = 0$ or $x = 0$. In the first case we get $vx = vz = 0$ or $z = x = 0$ by the assumption. In the second case follows from $vz = 0$ that $z = 0$.

4. $v = 0$ and from $tz = 0$ and $tx^* = 0$ follows that $t = 0$ or $x = z = 0$

4.1 $t = 0$, from $sx^* = sz^* = 0$ follows that either $s = t = v = 0$ or $x = z = 0 = y$, but $y \neq 0$ by assumption.

4.2 $x = z = 0$, from $ty = sy = 0$ follows that $s = t = v = 0$.

This concludes the proof.

1.2.5   A numerical approach

In this section we give an example of a numerical approach to the separability problem. Gurvits [110] reformulated the separability problem as a weak membership problem (allowing some error in the decision) and showed that even in this scenario the problem is NP-hard. Yet, as demonstrated by the partial transpose criterion, this does not exclude the existence of efficient algorithms for low dimensional systems. There have been several algorithmic proposals, which can be categorised in three classes:

From the outside Here a hierarchy of tests is devised which in every step detects entanglement of some states and provide a corresponding witness. Typically the first tests will detect highly entangled states, while further tests will detect more weakly entangled states. Ideally, the hierarchy should be complete, i.e. in the asymptotic regime every entangled state should be detected. Examples of such algorithms can be found in Ref. [32, 35, 74, 75, 76].

From the inside In this approach, again a hierarchy of tests is devised, but this time able to deliver a certificate for separability. States detected in the first tests will be typically close to the maximally mixed state, while further tests will be able to detect states closer to the boundary of entangled states. The logic behind this is that for weakly (classical) correlated states there is more freedom in finding a convex decomposition in terms of product vectors. Examples of such algorithms can be found in Ref. [159, 325].

Distance measure The starting point here is to take an entanglement measure $E(\rho)$ which satisfies $E(\rho) = 0$ for all separable states and $E(\rho) > 0$ for all entangled states. Examples of such measures include the entanglement of formation [21], and geometric measures such as the best separable approximation [182] (see

Section 3.3 for an introduction to entanglement measures). The algorithm typically works then by calculating $E(\rho)$ to a certain accuracy. For examples see Ref. [93, 182].

An exhaustive review on algorithms for the separability problem, with particular emphasis on comparing the different complexities of the algorithms, can be found in Ref. [162].

The most successful algorithms as of today use of optimisation theory, and in particular semidefinite programming. Semidefinite programs (SDPs) are convex optimisation problems which can be written as the minimisation of a linear object function, subject to semidefinite constraints in the form of linear matrix inequalities [32]:

$$\text{minimise} \quad c^T x,$$
$$\text{subject to} \quad F_0 + \sum_i x_i F_i \geq 0,$$

where $\{x_i\}$ is a finite set of real variables, c a constant vector and F_i some fixed Hermitian matrices. Semidefinite programs have two appealing features. Firstly, efficient algorithms are available for solving SDPs in polynomial time with arbitrary accuracy. Secondly, with each (primal) SDP there is associated a dual SDP:

$$\text{maximise} \quad - \text{Tr}[F_0 Z],$$
$$\text{subject to} \quad \text{Tr}[F_i Z] = c_i, \quad Z \geq 0$$

Here $Z \geq 0$ means that Z is a positive semi-definite (Hermitian) operator. Now it is not so hard to see that $c^T x$ is always larger than $- \text{Tr}[F_0 Z]$, so that solving the dual problem gives a lower bound on the primal problem. It is often the case that these values coincide, in which case the SDP's have the so-called strong duality property. Suppose now that $c = 0$, then the primal problem becomes a feasibility problem. Then a positive value of $- \text{Tr}[F_0 Z]$ shows that the primal problem is not feasible. In other words the operator Z gives a certificate for the infeasibility. Needless to say that such certificates are of great value in decision problems such as the separability problem.

The two most important algorithms that use SDP, as of today, are the algorithms of Eisert et. al. [93] and Doherty et. al. [75]. The first approach is based on calculating the distance of a state to the set of separable states. In first instance this leads to a global

minimisation problem with polynomial constraints. Using Lasserre's method of semi-definite relaxations, this can then be reformulated as a sequence of SDPs. The hierarchy of tests obtained is complete, as every entangled state will be found at some stage in the hierarchy. Since a global optimum will be found at some point also separability can be detected [89].

Doherty's approach is based on the existence of symmetric extensions for separable states. It works from the outside and is also complete; furthermore, when a state is found to be entangled, the dual problem yields a corresponding entanglement witness. These entanglement witnesses turn out to have interesting algebraic properties, which is why we will say a bit more about (without proofs though).

Suppose a state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable, then we know that it can be written as $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i| \otimes |\phi_i\rangle\langle\phi_i|$. With ρ, we can associate the following state:

$$\tilde{\rho} = \sum_i p_i |\phi_i\rangle\langle\phi_i| \otimes |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$$

on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_A$. This extension is naturally symmetric under interchange of the first and third party. It also has positive partial transposition (with respect to any subsystem) and by tracing out the third party, we recover the original state. An extension for an arbitrary state satisfying these three properties will be called a symmetric extension. Equally, we can consider a symmetric extension with 2 copies of the first party. Using de Quantum de Finetti theorem one can prove the following characterisation of separable states:

Theorem 1.2.12. *A state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable if and only if it has a symmetric extension to any number of copies of subsystem A.*

Apparently this theorem has been around for some time, see Ref. [75] for its history. The new result by Doherty et. al. was to show that the feasibility problem of finding a symmetric extension to a fixed number of k copies can be cast into a semidefinite program. In this way, one obtains a hierarchy of tests, in which each test is stronger than the other. Indeed, when an extension to $k + 1$ copies exist, then naturally an extension to k copies exists. The first test is the usual partial transpose criterion, while further tests go beyond that and are able to detect PPT entangled states. In practice, it turns out that the algorithm detects all known PPT entangled states in the second

test of the hierarchy. The only major disadvantage is, that in practice, it is limited to density matrices acting on $\mathcal{H}$ with $\dim \mathcal{H} \leq 36$ because of memory constraints of existing implementations.

If the primal problem fails, the dual problem yields a corresponding entanglement witness. In Theorem 1.2.9 we have seen that when a positive map Λ_W with real coefficients is decomposable, then the associated real biquadratic form can be written as a SOS of linear forms. This result readily generalises to arbitrary positive maps. Now remarkably we have the following [75]:

Theorem 1.2.13. *Let $E_W(x, y)$ be the bihermitian form associated with an entanglement witness W obtained from the $(k + 1)th$ test of the hierarchy. Then $F(x, y) = \langle x|x \rangle^k E_W(x, y)$ can be written as a SOS.*

With this one can prove [75] the following characterisation of entanglement witnesses.

Corollary 1.2.2. *Let W be an entanglement witness in the interior of the set of entanglement witnesses (that is $\mathrm{Tr}(\rho_{sep} W) > 0$ for all separable ρ_{sep}). Then there is a $k > 0$ such that*

$$F(x, y) = \langle x|x \rangle^k E_W(x, y)$$

is a SOS.

Note that a similar characterisation can be deduced from it for positive maps. As an example consider the Størmer state σ given by (1.9), detected by Choi's map Λ_C (1.8). The second test of the hierarchy yields just the entanglement witness W_C associated with Λ_C and provides the SOS form for it:

$4\langle xy|W_C|xy \rangle \langle x|x \rangle = |2x_0 x_0^* y_0 - 2x_1 x_0^* y_1 + x_1 x_1^* y_0 - x_2 x_0^* y_2|^2 + 3|x_2 x_1^* y_2 - x_1 x_1^* y_1|^2 +$

$3|y_0 x_1 x_1^* - x_2 y_2 x_0^*|^2 + 3|x_2 x_2^* y_2 - x_0 x_2^* y_0|^2 + |2x_0 x_1 y_2^* - x_2 x_0 y_1^* - x_1 x_2 y_0^*|^2 +$

$3|x_0 x_2 y_1^* - x_1 x_2 y_0^*|^2 + |2x_0 x_0^* y_2 - 2x_1 x_2^* y_1 + x_2 x_2^* y_2 - x_0 x_2^* y_0|^2 +$

$|2x_0 x_1^* y_0 - 2x_2 x_2^* y_1 + x_2 x_1^* y_2 - x_1 x_1^* y_1|^2 \geq 0.$

1.3   Permutation criteria

1.3.1   From cross norm over realignment to permutation criteria

In this section we will introduce a class of separability criteria, known as the permutation criteria. We will introduce them in the way they have historically been found. Our starting point is a characterisation of separable states known as the cross norm criterion [249]. The greatest cross norm $\|\cdot\|_\gamma$ is defined on operators in $\rho \in \mathcal{L}_{\mathcal{H}_A} \otimes \mathcal{L}_{\mathcal{H}_B}$ as

$$\|\rho\|_\gamma = \inf_{u_i,v_i} \left[\sum_i \|u_i\| \cdot \|v_i\| \,\middle|\, \rho = \sum_i u_i \otimes v_i \right],$$

where $\|A\| = \mathrm{Tr}[(AA^\dagger)^{1/2}]$ is the trace norm (sum of the singular values). With this Rudolph [249] proved the following theorem.

Theorem 1.3.1. *Let ρ be a density operator on $\mathcal{H}_A \otimes \mathcal{H}_B$. Then ρ is separable if $\|\rho\|_\gamma = 1$ and entangled if $\|\rho\|_\gamma > 1$.*

The proof is technical and we omit it here. Note that the difference $\|\rho\|_\gamma - 1$ satisfies all the usual basic requirements for an entanglement measure [250]. Unfortunately the greatest cross norm is in practice, with the exception of highly symmetrical states, very hard to calculate.

One can equally well define other cross norms, by using a different norm in the definition. Let us denote by $\|\cdot\|_g$ the cross norm induced by the Hilbert-Schmidt norm $\|A\|_2 = [\mathrm{Tr}(AA^\dagger)]^{1/2}$. From $\|\rho\|_g \leq \|\rho\|_\gamma$[4] follows that a state ρ with $\|\rho\|_g > 1$ is entangled. It turns out that $\|\rho\|_g$ is easily computable, the construction is the following ([251, 254], see also [58]).

In Section 1.2.2 we have seen an isomorphism between vectors $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and operators $\Psi \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ defined by

$$|\psi\rangle = \sqrt{d}(\Psi \otimes \mathbb{1})|\psi_+\rangle = \sqrt{d}(\mathbb{1} \otimes \Psi^T)|\psi_+\rangle.$$

The space $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ is a Hilbert space, when furnished with the Hilbert-Schmidt inner product $\mathrm{Tr}(\Psi^\dagger \Phi)$ for $\Psi, \Phi \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$. It follows that the isomorphism is a

---

[4]This is because $\|\cdot\|_\gamma$ majorizes any unitarily invariant norm (hence the name greatest cross norm).

Hilbert-space isomorphism, i.e. isometric as $\langle \psi | \phi \rangle = \mathrm{Tr}(\Psi^\dagger \Phi)$. Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and $\rho \in \mathcal{L}(\mathcal{H})$. We can decompose ρ arbitrarily as

$$\rho = \sum_i u_i \otimes v_i$$

with $u_i \in \mathcal{L}(\mathcal{H}_A)$ and $v_i \in \mathcal{L}(\mathcal{H}_B)$. Now we apply the above isomorphism to both u_i and v_i and obtain

$$|\rho\rangle = \sum_i |u_i\rangle \otimes |v_i\rangle,$$

with $|\rho\rangle \in \mathcal{H} \otimes \mathcal{H}$. Applying the isomorphism on $|\rho\rangle$ we obtain

$$R(\rho) = \sum_i |u_i\rangle\langle v_i|.$$

The operator $R(\rho) \in \mathcal{L}(\mathcal{H})$ is independent of the chosen decomposition of ρ and in general $\rho \neq R(\rho)$. This is because we can interpret $|\rho\rangle = |\rho\rangle_{1234} \in \mathcal{H} \otimes \mathcal{H}$ as an element of $(\mathbb{C}^d)^{\otimes 4} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4$, then with ρ acting on $\mathcal{H}_1 \otimes \mathcal{H}_3$ we have

$$|\rho\rangle = \sum_{i,j=1}^{d} (\rho_{13} \otimes \mathbb{1}_{24})|\psi_+\rangle_{13|24},$$

as opposed to

$$|\rho\rangle = \sum_{i,j=1}^{d} (R(\rho_{12}) \otimes \mathbb{1}_{34})|\psi_+\rangle_{12|34}.$$

Here $|\psi_+\rangle_{13|24}$ denotes the maximally entangled state with respect to the $13|24$ division (and analogue for $|\Psi_+\rangle_{12|34}$). The next lemma is a well known identity from the theory of operator norms (see e.g. [258])

Lemma 1.3.1. *For any operator $R \in \mathcal{L}(\mathcal{H})$ we have*

$$\|R\| = \inf_{u_i, v_i} \left[\sum_i \sqrt{|\langle u_i | u_i \rangle|} \cdot \sqrt{|\langle v_i | v_i \rangle|} \,\middle|\, R = \sum_i |u_i\rangle\langle v_i| \right].$$

With this lemma, we can prove that $\|R(\rho)\| = \|\rho\|_g$ and from that we obtain an easily computable necessary criterion for separability:

Theorem 1.3.2 (Realignment criterion)**.** *For any state $\rho \in \mathcal{L}(\mathcal{H})$ the identity*

$$\|R(\rho)\| = \|\rho\|_g$$

holds. If $\|R(\rho)\| > 1$, then ρ is entangled.

Proof. Let $\rho = \sum_i u_i \otimes v_i$, then $\sqrt{|\langle u_i | u_i \rangle|} = \sqrt{\text{Tr}(u_i^\dagger u_i)} = \|u_i\|_2$ (and similar for v_i). The theorem then follows from the previous lemma together with the definition of $\| \cdot \|_g$ and inequality $\|\rho\|_g \leq \|\rho\|_\gamma \leq 1$ for separable states ρ. $\square$

From the discussion above it follows that $R(\rho)$ is nothing more then a rearrangement of matrix entries of ρ. For this reason, it is often referred to as the realignment criterion [44, 218, 252]. Some analytical properties of the realignment criterion have been studied in Ref. [253]. It turns out that the realignment criterion is independent of the partial transposition and hence can detect PPT entangled states. From our discussion it is easy to see that the realignment criterion corresponds to the operation R which acts on basis states as

$$|\psi_i\rangle\langle\psi_j| \otimes |\psi_k\rangle\langle\psi_l| \xrightarrow{R} |\psi_i\rangle\langle\psi_k^*| \otimes |\psi_j^*\rangle\langle\psi_l|.$$

Due to linearity, this operation is well defined for arbitrary quantum states. The partial transposition is also based on reordering of matrix entries. In the same notation, we denote it as the operation T which acts on the second subsystem as

$$|\psi_i\rangle\langle\psi_j| \otimes |\psi_k\rangle\langle\psi_l| \xrightarrow{T} |\psi_i\rangle\langle\psi_j| \otimes |\psi_l^*\rangle\langle\psi_k^*|.$$

A state ρ is entangled if the trace norm $\|T(\rho)\| > 1$. Note that the usual partial transpose criterion says that a state is entangled if $T(\rho)$ has some negative eigenvalues, but as $T(\rho)$ is Hermitian this is equivalent to saying that $\|T(\rho)\| > 1$. This was first observed in Ref. [305], where it was shown that the quantity $\|T(\rho)\|$ gives rise to a good entanglement measure (see also [45]).

This striking similarity between the two criteria led to the consideration of general permutations of multipartite density matrices [144]. Consider an r-party state belonging to a Hilbert space $\mathcal{H}$, whose subsystems have the same dimension d. A general state $\rho \in \mathcal{H}$ can be expanded as

$$\rho = \sum_{i_1, i_2, \ldots, i_{2r}} \rho_{i_1 i_2, i_3 i_4, \ldots, i_{2r-1} i_{2r}} |i_1 i_3 \ldots i_{2r-1}\rangle\langle i_2 i_4 \ldots i_{2r}|,$$

where all indices run from 1 to d. Let S_{2r} denote the symmetric group with $(2r)!$ elements, that is, the group of the permutations of the set $\{1, 2, \ldots, 2r\}$. We define for each permutation $\sigma \in S_{2r}$ a corresponding map Λ_σ on operators acting on $\mathcal{H}$ as

$$\left[\Lambda_\sigma(\rho)\right]_{i_1 i_2, \ldots, i_{2r-1} i_{2r}} = \rho_{i_{\sigma(1)} i_{\sigma(2)}, \ldots, i_{\sigma(2r-1)} i_{\sigma(2r)}}. \tag{1.12}$$

We will represent permutations as $[\sigma(1)\,\sigma(2)\,\ldots\,\sigma(2r)]$ or in disjoint cycles. With this notation the partial transpose criterion corresponds to the permutation $[1\,2\,4\,3] = (3,\,4)$ while the realignment criterion corresponds to the permutation $[1\,3\,2\,4] = (2,\,3)$.

Theorem 1.3.3 (Permutation criteria for separability [144])**.** *Let ρ be a r-party state acting on a Hilbert space ρ and $\sigma \in S_{2r}$ an arbitrary permutation. If*

$$\|\Lambda_\sigma(\rho)\| > 1,$$

with $\|\cdot\|$ the trace norm, then ρ is entangled (that is, not fully separable).

Proof. Let ρ be a fully separable state on $\mathcal{H}$, that is

$$\rho = \sum_i p_i |\psi_1^i\rangle\langle\psi_2^i| \otimes |\psi_3^i\rangle\langle\psi_4^i| \otimes \ldots |\psi_{2r-1}^i\rangle\langle\psi_{2r}^i| = \sum_i p_i \rho_i,$$

with $\psi_{2k-1}^i = \psi_{2k}^i$ and ρ_i the corresponding pure states. Then $\Lambda_\sigma(\rho)$ corresponds to

$$\Lambda_\sigma(\rho) = \sum_i p_i |\psi_{\sigma(1)}^{i\#}\rangle\langle\psi_{\sigma(2)}^{i\#}| \otimes |\psi_{\sigma(3)}^{i\#}\rangle\langle\psi_{\sigma(4)}^{i\#}| \otimes \ldots |\psi_{\sigma(2r-1)}^{i\#}\rangle\langle\psi_{\sigma(2r)}^{i\#}| = \sum_i p_i \Lambda_\sigma(\rho_i),$$

with $\psi_k^{i\#} = \psi_k^{i*}$ if $\sigma(i)$ and i have different parity and $\psi_k^{i\#} = \psi_k^i$ otherwise. We need to show that $\|\Lambda_\sigma(\rho)\| \leq 1$, but because of $\|A + B\| \leq \|A\| + \|B\|$ it is sufficient to show that $\|\Lambda_\sigma(\rho_i)\| \leq 1$. But this follows easily from $\|A \otimes B\| \leq \|A\|\|B\|$ and $\||\phi\rangle\langle\psi|\| = 1$ for normalised vectors $|\phi\rangle$ and $|\psi\rangle$. $\square$

As a corollary we will show here how to construct an entanglement witness for a r-party state ρ given that $\|\Lambda_\sigma(\rho)\| > 1$ for some permutation σ. For this we generalise the bipartite construction of Chen and Wu in Ref. [55], see also Ref. [109, 145, 332]. Here and elsewhere permutations are evaluated from *left* to *right*.

Theorem 1.3.4. *Let $\|\Lambda_\sigma(\rho)\| > 1$ for some permutation σ, and define*

$$\tilde{\sigma} = \tau\sigma^{-1}\tau$$

with τ the global transposition and σ^{-1} the inverse permutation of σ. Then

$$W = \mathbb{1} - \Lambda_{\tilde{\sigma}}(VU^\dagger)$$

is an entanglement witness with $\mathrm{Tr}(\rho W) = 1 - \|\Lambda_\sigma(\rho)\| < 0$. Here U and V are the unitary matrices corresponding to the singular value decomposition of $\Lambda_\sigma(\rho) = UDV^\dagger$.

Proof. It is straightforward to check that $\mathrm{Tr}(\rho W) = 1 - \|\Lambda_\sigma(\rho)\|$ from the identity

$$\mathrm{Tr}[A\Lambda_\sigma(B)] = \mathrm{Tr}[(\Lambda_{\sigma^{-1}}(A^T))^T B] = \mathrm{Tr}[\Lambda_{\tilde\sigma}(A)B],$$

for arbitrary operators A and B. This identity can be verified by explicitly writing the trace as a sum over matrix indices.

Now all that is left is to show that W is positive on separable states. We will use of the following variational characterisation of the trace norm (see for instance [127], p195):

$$\|A\| = \max\{|\mathrm{Tr}(XAY)| \,|\, XX^\dagger = YY^\dagger = \mathbb{1}\}, \tag{1.13}$$

for arbitrary A. Let ρ_{sep} be an arbitrarily separable state, then

$$\|\Lambda_\sigma(\rho_{\mathrm{sep}})\| = \mathrm{Tr}(D') \le 1,$$

with $\Lambda_\sigma(\rho_{\mathrm{sep}}) = U'D'V'^\dagger$ the singular value decomposition of $\Lambda_\sigma(\rho_{\mathrm{sep}})$. From (1.13) follows that $\mathrm{Tr}[X\Lambda_\sigma(\rho_{\mathrm{sep}})Y]$ is maximal when $X = U'$ and $Y = V'^\dagger$ and thus

$$\begin{aligned}
\mathrm{Tr}(W\rho_{\mathrm{sep}}) &= 1 - \mathrm{Tr}(\Lambda_{\tilde\sigma}(VU^\dagger)\rho_{\mathrm{sep}}) \\
&= 1 - \mathrm{Tr}(U^\dagger\Lambda_\sigma(\rho_{\mathrm{sep}})V) \\
&\ge 1 - \mathrm{Tr}(U'\Lambda_\sigma(\rho_{\mathrm{sep}})V'^\dagger) \\
&= 1 - \|\Lambda_\sigma(\rho_{\mathrm{sep}})\| \ge 0.
\end{aligned}$$

$\square$

For an r-party state, there are $(2r)!$ permutation criteria, but not all of them are inequivalent. For instance for bipartite systems it is easy to see that partial transposition with respect to the first system is equivalent to the partial transposition with respect to the second. For bipartite systems all permutation criteria turn out to be equivalent to either the partial transposition or the realignment criterion [144]. For more than two parties the classification of inequivalent permutation criteria is an open problem. First steps toward such a classification have been made in Ref. [96, 144, 324]. For three parties it was implied that there are 9 inequivalent criteria [96, 324], and for four parties at most 34 inequivalent criteria [324].

In the next section we define exactly what we mean by independent criteria and review the work of Wocjan and Horodecki [324] on so-called combinatorially independent permutation criteria and introduce their graphical notation. Then we point out that both papers [96, 324] overlooked an obvious fact. We show that for three parties there are just 6 independent criteria and 22 for four parties. We prove that the class of the combinatorially independent permutation criteria contains some equivalent criteria which always occur in pairs. We completely classify these criteria and give a new upper bound of the number of independent criteria (this is Theorem 1.3.7). It will become clear that most likely there are no more equivalences in the remaining criteria, although we were unable to provide a complete proof of this. A proof is presented for 2, 3 and 4 parties and numerical evidence for up to 8 parties is given. These results were first published in Ref. [63].

1.3.2   Definitions, graphical notation and first results

Let σ and μ be two permutations in S_{2r}. We call the corresponding entanglement criteria σ and μ dependent if and only if

$$\|\Lambda_\sigma(\rho)\| = \|\Lambda_\mu(\rho)\|, \tag{1.14}$$

for all quantum states. Else, the permutation criteria are called independent. Observe that if two permutation criteria σ and μ are independent by the above definition, it could still be that they detect exactly the same entangled states. This would occur if we had

$$\|\Lambda_\sigma(\rho)\| > 1 \quad \Leftrightarrow \quad \|\Lambda_\mu(\rho)\| > 1$$

for all quantum states ρ. However, as we will see in the next section, the condition in (1.14) is already good enough to reduce significantly the number of permutation separability criteria. Furthermore, we prove later that the criteria which are independent are also truly independent (in the sense that no criterion is strictly stronger than any other) for up to four subsystems.

Our necessary condition extends the necessary condition of combinatorial independence introduced in Ref. [324]. The definition of combinatorial independence is similar to the definition of independence. The decisive difference is that two permutations are

combinatorially dependent if and only if equality in (1.14) is achieved for *all* operators and not only quantum states. In this case, it is easy to see that the maps Λ_σ and Λ_μ are related by a norm-preserving map Λ. That is $\Lambda_\sigma(A) = \Lambda(\Lambda_\mu(A))$ with $\|A\| = \|\Lambda(A)\|$ for all operators A. Moreover, it can be shown that if Λ_σ and Λ_μ are related via a norm-preserving map Λ, then $\Lambda = \Lambda_\nu$ must come from some permutation ν. We call such a permutation a norm-preserving permutation.

An example of such a norm-preserving permutation is the global quantum transpose (GQT), which transposes the complete system. It can be written as

$$\tau = (1,2)(3,4)\cdots(2r-1,2r).$$

Another example of a norm preserving map Λ is the unitary transformation $\Lambda(\rho) = U\rho V$, where U and V are unitary operators. Reordering the different parties in the density matrix representation is an example of such a unitary transformation. Consider for instance the transformation

$$\rho = \sum_i \rho_i^A \otimes \rho_i^B \to \rho' = \sum_i \rho_i^B \otimes \rho_i^A.$$

This mapping can be implemented by means of multiplication on the left and on the right by the swap operator [324].

To illustrate the necessary condition of combinatorial independence let us consider again a bipartite system. The operation R' induced by the permutation $(1, 4)$ gives rise to the same criterion as R induced by the permutation $(2, 3)$. Indeed, the permutation $R'\tau$ transforms $[1\,2\,3\,4]$ into $[2\,4\,1\,3]$, which up to reordering of the parties is equivalent to $[1\,3\,2\,4]$. This is just the transformation defined by R.

Theorem 1.3.5 (Combinatorially independent criteria [324]). *The group $\mathcal{T}$ of norm preserving permutations can be generated as*

$$\mathcal{T} = \langle (2k, 2l), (2k-1, 2l-1), \tau \rangle,$$

where $1 \le k, l \le r$ and τ as before denotes the GQT. The combinatorially independent permutation criteria correspond to the right cosets $S_{2r}/\mathcal{T}$ of $\mathcal{T}$ in S_{2r}. The number of independent permutation criteria is therefore not larger than $\frac{1}{2}\binom{2r}{r}$. In this number, the class of trivial norm preserving criteria is also counted.

graphical representation	corresponding permutation	name
$k \quad \bullet \longrightarrow \bullet \quad l$	$(2k,\ 2l-1)$	reshuffle R_{kl}
$k \quad \bullet \longleftarrow \bullet \quad l$	$(2k-1,\ 2l)$	reshuffle R'_{lk}
$k \quad \circlearrowleft$	$(2k-1,\ 2k)$	partial transpose
$k \quad \bullet$	$()$	identity

Figure 1.3: Basic permutations, $k < l$ (Table from Ref. [324]).

In the same paper, the authors also devised a graphical notion of the criteria, which leads to a way of selecting a simple representative for the right cosets. They decompose any permutation as a combination of 4 elementary permutations: the partial transpose, two types of realignment or reshuffling, and the identity. The corresponding graphical notations are loops from a subsystem to itself, arrows from one subsystem to another and free subsystems (no loops or arrows), as graphically depicted in Figure 1.3. We call k the head and l the tail if there is an arrow from k to l. If there is a loop in m, then m is both head and tail of the loop. We call the support of an arrow or a loop the set containing its head and tail. A configuration of arrows and loops is called disjoint, if the supports of all pairs and loops are disjoint.

Theorem 1.3.6 (Canonical representation of combinatorially independent criteria [324]). *The right cosets $S_{2r}/\mathcal{T}$ can always be represented by a disjoint configuration of arrows, that is, they can be decomposed as a combination of the 4 elementary permutations. It is always possible to represent a random permutation $\sigma \in S_{2r}$ by a disjoint configuration by applying the following consecutive rules*

Rule 1: Pruning *Writing σ as a product of disjoint cycles, we can prune all cycles of σ such that there are no adjacent even or odd numbers.*

Rule 2: Chopping *We can chop up σ into disjoint transpositions.*

Rule 3: Exchanging heads *By exchanging heads we then obtain a disjoint configuration of arrows.*

Rule 4: GQT *By reversing the direction of all arrows and replacing loops by free subsystems and vice versa we obtain an equivalent disjoint permutation.*

All criteria that can be represented by a disjoint configuration of arrows are combinatorially independent up to a application of Rule 4, and possible application of Rule 3.

This theorem differs slightly from the corresponding one in the original paper [324]. They claimed that any two permutations represented by disjoint configurations are independent, up to application of Rule 4. As the following example illustrates, this is not always the case: by exchanging heads of $[1\,3\,2\,4\,5\,7\,6\,8]$ we obtain $[1\,7\,6\,4\,5\,3\,2\,8]$, which can be represented by a different disjoint configuration. And both configurations are not related via the GQT.

1.3.3   Main theorem

It was shown in Ref. [324] that two permutations μ and σ are combinatorially dependent if there is a norm preserving permutation such ν that $\Lambda_\sigma(A) = \Lambda_\nu(\Lambda_\mu(A))$ for all operators A. One could assume that therefore Theorem 1.3.5 cannot be sharpened, that is, that all combinatorially independent criteria are independent. This is true when one considers the permutation acting on arbitrary operators. In quantum mechanics however, we deal with positive operators, which are Hermitian. The following theorem exploits this fact and counts the new upper bound to the number of independent criteria.

Theorem 1.3.7. *(i) The permutation criteria corresponding to the permutations σ and $\tau\sigma$ are dependent.*

(ii). Let $\mathcal{Z} := \{e, \tau\}$ be the subgroup of S_{2r} generated by the GQT τ. Define the action of $\mathcal{Z}$ on the right cosets $S_{2r}/\mathcal{T}$ by multiplication from the left of the cosets, that is, $e * \sigma\mathcal{T} = e\sigma\mathcal{T}$ and $\tau * \sigma\mathcal{T} = \tau\sigma\mathcal{T}$. The new upper bound on the number of independent criteria is the number of orbits under this action. It is given by [5]

$$\frac{1}{4}\left[\binom{2r}{r} + 2^r + \binom{r}{r/2} \cdot even(r)\right],\tag{1.15}$$

where $even(r) = 1$ if r is even and 0 otherwise. This number includes the trivial criterion given by the identity permutation.

---

[5]The integer sequence generated by the number of independent criteria equals the integer sequence A045723 from Ref. [272].

Proof. To prove (i), let us apply the permutation $\tau\sigma$ on an arbitrary quantum state ρ. We have

$$
\begin{aligned}
\|\Lambda_{\tau\sigma}(\rho)\| &= \|\Lambda_\sigma(\Lambda_\tau(\rho))\| \\
&= \|\Lambda_\sigma(\rho^T)\| \\
&= \|\Lambda_\sigma(\bar\rho)\| \\
&= \|\overline{\Lambda_\sigma(\rho)}\| \\
&= \|\Lambda_\sigma(\rho)\|.
\end{aligned}
\tag{1.16}
$$

Here we have used that $\rho^T = \bar\rho$ because ρ is Hermitian and $\Lambda_\sigma(\bar\rho) = \overline{\Lambda_\sigma(\rho)}$ because Λ only permutes the entries of the matrix.

Observe that multiplying a coset $\sigma\mathcal{T}$ by τ from the left is the same as conjugating it by τ because τ is contained in $\mathcal{T}$, that is, we have

$$
\tau\sigma\mathcal{T} = \tau\sigma\mathcal{T}\tau.
$$

It is readily verified that conjugation of a permutation by τ corresponds to exchanging heads (always odd numbers) and tails (always even numbers). Therefore, the direction of all (true) arrows is reversed and loops and free subsystems are not affected. An example is shown in Figure 1.4. Following the four rules presented in Ref. [324], we call this Rule 5. The new rule either *glues* two criteria together or does not change them. More precisely, the orbits under the action of $\mathcal{Z}$ have size 1 or 2. The orbit of size two is generated by the involution τ:

$$
\sigma\mathcal{T} \to \tau\sigma\mathcal{T} \to \tau\tau\sigma\mathcal{T} = \sigma\mathcal{T}.
$$

(ii). There are $\frac{1}{2}\binom{2r}{r}$ combinatorially independent criteria. With the new rule, there are at most

$$
\frac{1}{2}\binom{2r}{r} - \frac{1}{2}\left[\frac{1}{2}\binom{2r}{r} - K\right],
$$

independent criteria left. Here K denotes the number of criteria not affected by conjugating according to the new rule. Now note that the only criteria (represented as disjoint arrow configurations) not affected by conjugation with τ are

1. criteria with no arrows and

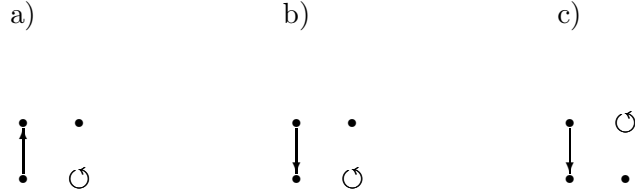a)   b)   c)

Figure 1.4: Action of the new rule on a disjoint arrow configuration: our new rule changes a) to b). Compare this with the action of rule 4 in Ref. [324] which changes a) to c). Our new rule only reverses the direction of true arrows, whereas rule 4 additionally creates loops on free subsystems and removes loops.

2. criteria containing only arrows and having no free subsystems.

If r is odd, then situation (2) cannot occur. The number of these criteria is readily counted:

$$\binom{r}{0} + \binom{r}{1} + \binom{r}{2} + \cdots + \binom{r}{\lfloor (r/2) \rfloor} = 2^{r-1},$$

where we have used an identity of binomial coefficients. So when the number of subsystems is odd, the number of criteria becomes (including the identity)

$$\frac{1}{4}\left[\binom{2r}{r} + 2^r \right].$$

In the case r is even we need to take care of situation (2). Now this number equals picking $r/2$ heads from r choices, because exchanging tails does not matter. But we have to divide by two since exchanging all heads and tails does not matter either, so that the number of criteria satisfying (2) is given by

$$\frac{1}{2}\left[\binom{r}{r/2} \right].$$

We conclude that when r is even, the number of criteria is given by (including the identity)

$$\frac{1}{4}\left[\binom{2r}{r} + 2^r + \binom{r}{r/2} \right].$$

To complete the proof, we have to show that the criteria in the orbits of size 2 are combinatorially independent. Let σ be a permutation represented by a disjoint arrow configuration. Assume that there is an arrow from subsystem k to l in the disjoint configuration of σ. Then there is an arrow from l to k in the disjoint configuration

describing $\tau\sigma\tau$. Loops and free subsystems are not affected. Using these observation we see that the configuration describing $\sigma\tau\sigma\tau$ has a closed path from k to l and no loops. The closed path between k and l can be transformed into a loop on k and a loop on l with the help of Rule 3 (Exchanging heads) in Ref. [324]. Now if we apply these arguments to all arrows of σ we see that the permutation $\sigma\tau\sigma\tau$ is not norm-preserving. Consequently, the permutations σ and $\tau\sigma\tau$ are combinatorially independent. This concludes the proof.   □

Figure 1.4 shows an example of how the new rule glues two combinatorially independent criteria together. In general, we have that two permutations corresponding to disjoint arrow configurations are related by the new rule if and only if they have the same (true) arrow structure (up to exchanging heads) and a complementary loop/free subsystem structure. The latter means that if the first criterion has a loop on subsystem k then the subsystem k is free in the second and vice versa.

1.3.4   Illustrations

The different criteria resulting from our characterisation for two, three and four parties are shown graphically in Figure 1.5. In this figure, we have adopted the simplified graphical notation of [324] without arrows. Loops (QT) have been denoted by a little circle, $(2k, 2l-1)$ permutations (R) as a solid line and $(2k-1, 2l)$ permutations (R') as a dotted line. In order to construct this figure one first draws all disjoint configurations, and then eliminates those related by application of Rules 3, 4 and 5.

Below we show that all listed criteria are *truly* independent, in the sense that no criterion detects strictly more states than any other criterion. A property we are going to use frequently is that the permutation criteria are insensitive to adding an uncorrelated ancilla. Let ρ be an r-party state and define the $r+1$-party state $\rho' = \rho \otimes \rho_{r+1}$. Suppose $\sigma \in S_{2r}$ and define $\sigma' = \sigma \in S_{2(r+1)}$, (the same permutation, but now acting on an enlarged set of $2(r+1)$ elements). Then from $\|\Lambda_{\sigma'}(\rho')\| = \|\Lambda_\sigma(\rho) \otimes \rho_{r+1}\| = \|\Lambda_\sigma(\rho)\|\|\rho_{r+1}\| = \|\Lambda_\sigma(\rho)\|$ follows that $\|\Lambda_\sigma(\rho)\| = \|\Lambda_{\sigma'}(\rho')\|$.

Figure 1.5: Independent permutation criteria for a) two, b) three, and c) four particles. The figure is adapted from Ref. [324].

Two parties

For a quantum system consisting of two parties, there are only two non trivial in-equivalent permutation criteria: the partial transpose in one of the subsystems and reshuffling between the two subsystems. For the low dimensional systems $\mathcal{H} \cong \mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathcal{H} \cong \mathbb{C}^2 \otimes \mathbb{C}^3$ the positivity of the partial transpose is a necessary and sufficient condition for separability [132], while this is not the case for the realignment criterion [44, 253]. For higher dimensional systems these criteria are truly independent, as there exist bound entangled states that are detected by the realignment criterion. As a curiosity, we have tested the realignment criterion on all known bound entangled states $\rho \in \mathcal{H} \cong \mathbb{C}^3 \otimes \mathbb{C}^3$ in the literature. The maximum value we have found for $\|R(\rho)\|$ is $7/6$ and is achieved for a particular chess-board state [38]:

$$\rho_c = \frac{1}{12} \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & -1 & 0 \\ 1 & 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{1.17}$$

Three parties

For three parties we have proven that at most 6 criteria are independent, previous work [96, 324] indicated that there were 9. The 6 criteria are the partial transposes (row QT) in the 3 subsystems and the 3 reshufflings (row R) between any of the two subsystems. On random states, it can easily be checked that the 6 criteria are indeed independent according to our definition; we now show that no criterion is strictly stronger than any other.

To show that the criteria from row QT are truly independent from one another, it is sufficient to note that there exist tripartite NPT states which are separable with regard to two splits, but not to the third one. An example of these kind of states for qubits can

be found in Ref. [82]. Such states will obviously be detected by only one criterion from
the row QT. To show the independence between the criteria in the row R, we use the
property (see also [253]) that the trace norm of the realigned density matrix remains
invariant when an uncorrelated ancilla is added. Now taking a bipartite entangled state
which violates the realignment criterion, and adding an uncorrelated ancilla, we find
that it is only detected by only one criterion from row R (since it is separable in the
other splits).

All what is left is to show that there are no dependences between the rows R and
QT. So let us take two arbitrary criteria, one from row R and one from row QT. Here
we can distinguish two cases, the first is where the realignment works on different
subsystems than the partial transposition. As an example let us take realignment R_{12}
between subsystem 1 and 2, and partial transposition QT_3 of subsystem 3. Let ρ be
a bipartite entangled state detected by both the realignment and the partial transpose
criterion. Then the state $\rho' = \rho \otimes \rho_3$, with ρ_3 an arbitrary state, will be detected by
R_{12}, but not by QT_3. Conversely the state $\rho'' = \rho_1 \otimes \rho$ will be detected by QT_3 but not
by R_{12}. The second case, is where the realignment works on a same subsystem as the
partial transposition, such as R_{12} and QT_1. To show their independence it is sufficient
to consider bipartite states that are detected by either R or QT (but not both), and
adding an uncorrelated ancilla.

Note that the realignment criterion, in contrast to the partial transpose criterion
can detect tripartite entangled states, that are separable under any bipartite cut. This
has been demonstrated experimentally in Ref. [144] with the tripartite bound entangled
states from Ref. [23].

Four parties

For four parties, there are at 22 non trivial independent permutation criteria. As for
three parties, it easy to show the independence of the criteria within a fixed row, by
starting from an entangled two or three party state and adding uncorrelated ancillas.
This is probably hardest to see for the row R+QT, so we illustrate this with an example.
Let us take the two criteria $R_{12}QT_3$ and QT_1R_{23} and let ρ_{23} be a bipartite entangled
state which is detected by the realignment criterion. The state $\rho_1 \otimes \rho_{23} \otimes \rho_4$ (with

ρ_1, ρ_4 arbitrary states) is detected by QT_1R_{23}, but not by $R_{12}QT_3$, as this criterion is equivalent to the criterion $R'_{12}QT_4$.

Let us now focus on the criteria which contain only partial transpositions. The rows QT and 2QT are easily shown to be independent by adding uncorrelated ancillas. As an example consider the criteria QT_1 and QT_{12}. Let ρ_{12} be an NPT state, and add an uncorrelated ancilla ρ_{34}; clearly this state will be detected by QT_1 only. Conversely, constructing a state as the tensor product of an NPT entangled state ρ_{24} and a separable state ρ_{13} will give a state only detected by QT_{12}. The independence between the criteria with only loops and the criteria with at least one realignment follows easily from their independence in the bipartite case. As before this is done simply by adding suitable uncorrelated ancillas.

To show true independence within the set of realignment criteria (rows R, R+QT, 2R and R+R'), let us first consider the rows R and R+QT. Again, we consider an example, whereas the other cases can be shown similarly. Consider the criteria R_{12} and QT_4R_{23}. Let ρ be a bipartite entangled state which is detected by the realignment criterion and σ a separable state. Then the state $\rho_{12} \otimes \sigma_{34}$ will be detected only by R_{12}, while $\sigma_{14} \otimes \rho_{23}$ only by QT_4R_{23}. As for the criteria 2R and R+R', consider the non-trivial case $R_{12}R_{34}$ and $R_{12}R'_{34}$. Their independence can be shown by applying the criteria to the 4-qubit states $\psi = (|1000\rangle + |1101\rangle)/\sqrt{2}$ and $\psi' = (|1000\rangle + |1110\rangle)/\sqrt{2}$ (the first is detected by $R_{12}R_{34}$ only, while the second by $R_{12}R'_{34}$ only). All that is left, is to show that the criteria from row R and R+QT are independent of the criteria from rows 2R and R+R'. Without loss of generality we can take one representative from the rows 2R and R+R', say $R_{12}R_{34}$ (the other criteria correspond to appropriately swapping the subsystems). It is easy to find states that are detected by the criteria in rows R or R+QT but not by $R_{12}R_{34}$. Consider for example the criterion $R_{12}QT_3$. One can verify that it will detect the entangled state $\rho = \rho_c \otimes \mathbb{1}/9$; while this state is not detected by criterion $R_{12}R_{34}$. Finally an example to show that the criterion $R_{12}R_{34}$ can detect states not detected by any criterion in the rows R or R+QT is given by $\rho = (3/4)\rho_c \otimes \rho_c + (1/4)\mathbb{1}/81$.

Final remarks

In Ref. [144] a powerful class of separability criteria was devised based on permutations. The class however contained many redundancies, and to give a complete characterization of the independent criteria is an open problem. In Ref. [324] a graphical representation for permutations together with rules for simplifying them were introduced based on a sufficient condition for two permutations to yield dependent criteria. This equivalence meant that two combinatorially dependent criteria yield the same value of the trace norm on all operators. Combinatorially, density operators have a prominent Hermitian symmetry, that is a global quantum transposition together with a complex conjugate. We have exploited this symmetry and we have shown how this led to the dependence of particular combinatorially independent criteria. It is unlikely that there are more dependences in the criteria from Theorem 1.3.7.

Density operators differ from arbitrary operators also because they have positive eigenvalues. But since permutations only reorder matrix entries, it is unlikely that this positiveness would lead to more criteria to be dependent. We have verified the independence of the criteria numerically on a random state (using the algorithm outlined in Ref. [342]) for 2 up to 8 parties. In Appendix A.1 we have reproduced the matlab program which implements a random permutation. In the same way as we illustrated for three and four parties, it is easy to see that the criteria with only loops (only partial transpositions) are independent. These criteria are independent from the ones having at least one realignment since those can detect bound entangled states. To prove the independence within the class of criteria with at least one realignment one could try to generalize the arguments from the previous section.

Schmidt number for mixed states

In this chapter we introduce the Schmidt number for mixed states [286], as a generalisation of the Schmidt rank for pure states. It can be thought of as a refinement of the entangled versus separable division, where the set of mixed states is decomposed into a whole series of nested convex sets. In the first section, we study briefly the use of Schmidt witnesses to characterise these sets [257]. In the succeeding sections we derive the corresponding characterisation in terms of positive maps [95, 286] and discuss a conjecture on the decomposability of these maps in $3 \otimes 3$.

Robustness measures quantify the extent to which entangled states remain entangled under mixing. In the final part of this chapter, we generalise the notion of robustness of entanglement [304] and introduce the Schmidt robustness and random Schmidt robustness [61]. The latter notion is closely related to the construction of Schmidt balls around the identity. In particular we derive upper and lower bounds to the Schmidt robustness for pure states. We present two conjectures, the first one is related to the radius of inner balls around the identity in the convex set of Schmidt number n-states. We also conjecture a class of optimal Schmidt witnesses for pure states.

2.1 Introduction and Schmidt witnesses

In Ref. [286] the notion of Schmidt rank $S(\psi)$ of pure bipartite states $|\psi\rangle$ was extended to the Schmidt number $S(\rho)$ of mixed states ρ as

$$S(\rho) = \min_{\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|} \max_i S(\psi_i).$$

Thus ρ acting on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is said to have Schmidt number n if there exists a decomposition of $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with all vectors $\{|\psi_i\rangle\}$ having Schmidt rank at most n, and there exists no such decomposition with all vectors having a Schmidt rank $n-1$ or lower. This definition coincides with the Schmidt rank when ρ is a pure state. It is clear that separable states have Schmidt number one, whereas entangled states have a Schmidt number larger than one. Recall that we denoted the set of separable states as $\mathcal{S}$, and the complete set of states as $\mathcal{D}$. We will denote the set of density operators that have Schmidt number n or less by $\mathcal{S}_n$. Sets of increasing Schmidt number are embedded into each other as

$$\mathcal{S} = \mathcal{S}_1 \subset \mathcal{S}_2 \subset \ldots \subset \mathcal{S}_d = \mathcal{D}.$$

The subsets $\mathcal{S}_i$ are all closed and convex by construction. The Schmidt rank of a pure state cannot increase under local operations and classical communication [190], and this holds true for the Schmidt number as well. Furthermore, the Schmidt number of a state is trivially invariant under local unitaries. This makes the Schmidt number k of a state ρ, or equivalently the logarithmic Schmidt number $\mathcal{N}(\rho) = \log k$ a legitimate measure of entanglement. Most surprisingly, Terhal and Horodecki [286] showed that $\mathcal{N}(\rho)$ is not an additive quantity, that is there exists states ρ with Schmidt number k, such that

$$\mathcal{N}(\rho^{\otimes n}) \neq n \log k,$$

so that in general all we can say is that

$$\mathcal{N}(\rho) \leq \mathcal{N}(\rho^{\otimes n}) \leq n\mathcal{N}(\rho).$$

For multipartite systems, there is no straightforward generalisation of the Schmidt decomposition. However there have been a number of proposals, both for pure and mixed states (see e.g. [40, 90]):

In analogy to entanglement witnesses the set of states in S_k can be characterised with the aid of the so-called Schmidt witnesses [39, 257]. We call a Hermitian operator W a Schmidt witness of class k (for short k-SW) if and only if

1. $\text{Tr}(W\sigma) \geq 0$ for all $\sigma \in S_{k-1}$,

2. There exists a $\rho \in S_k$ such that $\text{Tr}(W\rho) < 0$,

The existence of a k-SW for a Schmidt number k state follows directly from Theorem 1.2.2.

Corollary 2.1.1. *A state $\rho \in \mathcal{D}$ has Schmidt number k if and only if $\text{Tr}(\rho W_{k+1}) \geq 0$ for all Schmidt witnesses W_{k+1} of class $k+1$.*

In a completely similar way as the discussion in Section 1.2.3 on PPT entangled states and their witnesses, every Schmidt number k state can be decomposed as the convex sum of a Schmidt number $k-1$ state and a Schmidt number k edge state (see Theorem 1.2.7). Furthermore for every Schmidt number k edge state there is a canonical witness that detects the state and conversely, every k-SW can be written in a canonical form with the aid of an Schmidt number k edge state (see Theorem 1.2.8). Since the theorems and proofs are almost identical we will not reproduce them here.

Consider the following example [286] of a one-parameter set of states exhibiting all possible Schmidt numbers and a corresponding set of k-SWs.

Example 2.1.1. *Let P_+ be a maximally entangled state acting on a Hilbert space $\mathcal{H} \cong \mathbb{C}^d \otimes \mathbb{C}^d$ and the unnormalized isotropic states [131, 241] defined by*

$$\rho_\beta = \mathbb{1} + \beta P_+, \qquad with \qquad -1 \leq \beta \leq \infty. \tag{2.1}$$

The isotropic state ρ_β has Schmidt number n if and only if

$$\frac{d((n-1)d-1)}{d-(n-1)} < \beta \leq \frac{d(nd-1)}{d-n}.$$

The operators

$$W_n = \mathbb{1} - d/(n-1)P_+, \tag{2.2}$$

are n-SW and detect in an optimal way the Schmidt number of the states ρ_β.

Let us for a moment assume that W_n is indeed a n-SW . Then it is not so hard to verify that when $\beta > d(nd-1)/(d-n)$, ρ_β has Schmidt number $n+1$. The example then follows from a continuity argument, if we can show that for $\beta = d(nd-1)/(d-n)$ the state has Schmidt number n. This can be done by virtue of an explicit decomposition in terms of pure states [286]. Such a decomposition can be deduced from our results in Section 2.4. The fact that W_n is a n-SW follows readily from the next lemma [131, 286].

Lemma 2.1.1. *Define the fully entangled fraction of a state ρ as*

$$\mathcal{F}(\rho) = \max_\Psi \langle \Psi | \rho | \Psi \rangle,$$

where the maximum is taken over all maximally entangled states.

(a) For a pure state $|\psi\rangle$ the fully entangled fraction is given by

$$\mathcal{F}(\psi) = \frac{1}{d} \Big[\sum_{i=1}^{d} \lambda_i \Big]^2,$$

with λ_i the Schmidt coefficients of $|\psi\rangle$.

(b) For an arbitrary state with Schmidt number k or less we have

$$\mathcal{F}(\rho) \leq \frac{k}{d},$$

Proof. (a) See Ref. [131].

(b) Suppose we have a pure state $|\psi\rangle$ with Schmidt rank k, so the problem is to maximise

$$\Big[\sum_{i=1}^{k} \lambda_i \Big]^2$$

subject to

$$\sum_{i=1}^{k} \lambda_i^2 = 1.$$

We solve this using the method of Lagrange multipliers and define

$$\mathcal{L} = \Big[\sum_{i=1}^{k} \lambda_i \Big]^2 + \mu \Big[\sum_{i=1}^{k} \lambda_i^2 - 1 \Big].$$

An extremum can be found by solving

$$\frac{\partial \mathcal{L}}{\partial \lambda_i} = 0, \qquad \frac{\partial \mathcal{L}}{\partial \mu} = 0.$$

The first relation leads to $\mu = -k$, and thus $\sum_i \lambda_i = k\lambda_j$, squaring this equation and carrying out summation over j yields

$$\mathcal{F}(\rho) = \frac{1}{d}\Big[\sum_{i=1}^{k}\lambda_i\Big]^2 \leq \frac{k}{d}.$$

If the state is not pure, this inequality remains true, since a mixed state of Schmidt number k can be written as a convex combination of pure states of Schmidt rank k. $\square$

In Ref. [160] a connection was made between Schmidt witnesses and entanglement witnesses. The central idea in their construction can be deduced from the following more general lemma [60], of which special cases have appeared in the literature over the years [83, 177, 310] (see also the recent [227]).

Lemma 2.1.2. *Let σ be a positive operator with Schmidt number $N \geq 1$ acting on $\mathcal{H}_1 = \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$ and let η be an operator acting on $\mathcal{H}_2 = \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$ positive on states with Schmidt number KN. Then the operator $\sigma \otimes \eta$ acting on $\mathcal{H}_1 \otimes \mathcal{H}_2 \cong \mathcal{H}_A \otimes \mathcal{H}_B$ is positive on states with Schmidt number K.*

Proof. It is clear that it is sufficient to prove the lemma for pure states $\sigma = |\phi\rangle\langle\phi|$. So let

$$|\phi\rangle = \sum_{i=1}^{N} \phi_i |a_i\rangle_{A_1} |b_i\rangle_{B_1},$$

and take an arbitrary Schmidt rank K state

$$|\psi\rangle = \sum_{j=1}^{K} \psi_j |e_j\rangle_A |f_j\rangle_B.$$

Then we need to prove that $\mathrm{Tr}(|\psi\rangle\langle\psi|\sigma \otimes \eta) > 0$. This trace operation can be composed of tracing out the first pair, and then the second, as $\mathrm{Tr}(\cdot) = \mathrm{Tr}_2(\mathrm{Tr}_1(\cdot))$. Then making use of the identity $\mathrm{Tr}_1(C(A_1 \otimes B_2)) = \mathrm{Tr}_1(C(A_1 \otimes \mathbb{1}_2))B_2$ we have

$$\mathrm{Tr}(|\psi\rangle\langle\psi|\sigma \otimes \eta) = \mathrm{Tr}_2(\mathrm{Tr}_1(|\psi\rangle\langle\psi|(\sigma \otimes \mathbb{1}_2))\eta)$$

Now $\mathrm{Tr}_1(|\psi\rangle\langle\psi|(\sigma \otimes \mathbb{1}_2))$ is the projector onto the pure Schmidt rank KN state

$$|\gamma\rangle_2 = \langle\phi|\psi\rangle = \sum_{ij} \phi_i \psi_j \langle a_i|e_j\rangle\langle b_i|f_j\rangle \in \mathcal{H}_2$$

from which the lemma follows. $\square$

Let S be a given $(k+1)$-SW and $P_+^{(k)}$ a maximally k-level entangled state, then from the above lemma follows that the operator S' defined by

$$S' = P_+^{(k)} \otimes S,$$

is an entanglement witness. Thus by enlarging the Hilbert space, any SW can be mapped onto an entanglement witness; a trick which will come back in Chapter 4.

2.2 Main theorem

In this section we prove the main result on k-positive maps: the operators corresponding to k-positive maps via the Jamiołkowski isomorphism (see Section 1.2.2) are positive on Schmidt number k states and vice verse. This is a generalisation of Theorem 1.2.4. Then we derive a characterisation of $\mathcal{S}_k$ in terms of positive maps, similar to Theorem 1.2.5. We start this section by giving some alternative characterisations of positive maps.

Recall that a map $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ is a k-positive map if and only if it the induced map

$$\Lambda_k = \mathbb{1}_k \otimes \Lambda : \mathcal{L}_{\mathbb{C}^k} \otimes \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathbb{C}^k} \otimes \mathcal{L}_{\mathcal{H}_B}$$

is positive for $k \geq 1$. The next lemma characterises k-positive maps purely on their action on pure states with Schmidt rank at most k (see for instance Ref. [95]).

Lemma 2.2.1. *A Hermitian map* $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ *is k-positive if and only if*

$$(\mathbb{1}_k \otimes \Lambda)(|\psi\rangle\langle\psi|) \geq 0,$$

for all pure states $|\psi\rangle \in \mathbb{C}^k \otimes \mathcal{H}_A$ *with Schmidt rank at most k.*

Proof. Trivial. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

An improvement is made by the following lemma, which states that it is sufficient to test maximally entangled vectors of rank k. Ref. [72] contains a proof for $k = 2$. We present here an alternative, much shorter proof for general k.

Lemma 2.2.2. *A Hermitian map* $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ *is k-positive if and only if*

$$(\mathbb{1}_k \otimes \Lambda)(|\psi\rangle\langle\psi|) \geq 0$$

for all maximally entangled states $|\psi\rangle \in \mathbb{C}^k \otimes \mathcal{H}_A$.

Proof. Let $|\psi\rangle \in \mathbb{C}^k \otimes \mathcal{H}_A$ be an arbitrary state in Schmidt decomposition:

$$|\psi\rangle = \sum_{i=0}^{k-1} \lambda_i |e_i\rangle |f_i\rangle.$$

In view of the previous lemma we need to show that

$$D = (\mathbb{1}_k \otimes \Lambda)(|\psi\rangle\langle\psi|) \geq 0 \qquad \text{if and only if} \qquad \tilde{D} = (\mathbb{1}_k \otimes \Lambda)(|\tilde{\psi}\rangle\langle\tilde{\psi}|) \geq 0,$$

with

$$|\tilde{\psi}\rangle = \sum_{i=0}^{k-1} |e_i\rangle |f_i\rangle.$$

But this follows immediately from

$$D = (L \otimes \mathbb{1})\tilde{D}(L^\dagger \otimes \mathbb{1}),$$

with L the diagonal matrix such that $L_{ii} = \lambda_i$. $\qquad\square$

Now we are in the position to prove the following theorem by Uhlmann. The proof is from Ref. [286].

Theorem 2.2.1. *A Hermitian map $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ is k-positive if and only if*

$$\sum_{n,m=1}^{k} \mu_n \mu_m \langle b_n | \Lambda(|a_n\rangle\langle a_m|) | b_m \rangle \geq 0$$

for all orthogonal sets of vectors $\{|a_n\rangle\}_{n=1}^{k}$ and $\{|b_n\rangle\}_{n=1}^{k}$ with $\sum_{n=1}^{k} \mu_n^2 = 1$.

Proof. From the preceding lemma we have that a Hermitian map is k-positive if and only if

$$\langle \phi | (\mathbb{1}_k \otimes \Lambda)(|\psi\rangle\langle\psi|) | \phi \rangle \geq 0,$$

for all ϕ and ψ with Schmidt rank k and ψ maximally entangled. Using the Schmidt decomposition we set $\phi = \sum_i \mu_i |c_i b_i\rangle$ and $\psi = \sum_i |c_i a_i\rangle$ (note that this is always possible, since ψ is maximally entangled) and obtain

$$\sum_{i,j,n,m=1}^{k} \mu_n \mu_m \langle c_n b_n | \mathbb{1}_k \otimes \Lambda(|c_i a_i\rangle\langle c_j a_j|) | c_m b_m \rangle \geq 0$$

from which the theorem follows. $\qquad\square$

With this we can prove the main theorem, first published in Ref. [286].

Theorem 2.2.2. *A linear map* $\Lambda_W : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ *is k-positive if and only if the corresponding operator* W *acting on* $\mathcal{H}_A \otimes \mathcal{H}_B$ *is positive on states* ρ *acting on* $\mathcal{H}_A \otimes \mathcal{H}_B$ *with Schmidt number k or less (belonging to* $\mathcal{S}_k$*).*

Proof. Let

$$W = (\mathbb{1} \otimes \Lambda_W)(P_+),$$

we have to show that k-positivity is equivalent to

$$\mathrm{Tr}\, W\rho \geq 0, \tag{2.3}$$

for all $\rho \in \mathcal{S}_k$. It is sufficient to take ρ as a pure state of Schmidt rank k, that is,

$$\rho = \sum_{n,m=1}^{k} \mu_m \mu_n |a_m b_m\rangle\langle a_n b_n|.$$

With this (2.3) can be rewritten as

$$\sum_{n,m=1}^{k} \mu_m \mu_n \langle a_n b_n | W | a_m b_m \rangle \geq 0,$$

or

$$\sum_{i,j,n,m=1} \mu_m \mu_n \langle a_n | i \rangle \langle a_m | j \rangle \langle b_n | \Lambda(|i\rangle\langle j|) | b_m \rangle \geq 0. \tag{2.4}$$

Due to the linearity of Λ we have that $\Lambda(|a_n\rangle\langle a_m|) = \sum_{ij} \langle i|a_n\rangle\langle a_m|j\rangle \Lambda(|i\rangle\langle j|)$, or

$$\Lambda'(|a_n\rangle\langle a_m|) = \sum_{ij} \langle a_n|i\rangle\langle a_m|j\rangle \Lambda(|i\rangle\langle j|),$$

with $\Lambda' = \Lambda \circ R$, where R maps the vectors $|a_n\rangle$ to $|a_n^*\rangle$ where complex conjugation is performed with respect to the $\{|i\rangle\}$ basis. Therefore (2.4) is equivalent to

$$\sum_{n,m=1}^{k} \mu_n \mu_m \langle b_n | \Lambda'(|a_n\rangle\langle a_m|) | b_m \rangle \geq 0,$$

and it follows that Λ' is k-positive if and only if $\mathrm{Tr}\, W\rho \geq 0$ for all $\rho \in \mathcal{S}_k$. Now the map R corresponds to a unitary rotation which maps the basis $\{|a_n\rangle\}$ to the basis $\{|a_n^*\rangle\}$. Therefore Λ is k-positive if and only if Λ' is. $\qquad\square$

Thus in the language of Schmidt witnesses: A map is k-positive if and only the corresponding operator is a $k + 1$ Schmidt witness. As an example consider the $k + 1$-SW (2.2)

$$W_{k+1} = \mathbb{1} - \frac{d}{k}P_+,$$

the corresponding map is given by $\Lambda_k(X) = \text{Tr}(X)\mathbb{1} - kX$. The positivity properties of this map have been derived independently by Tomiyama [289] (see also Ref. [281]), but from our correspondence they follow directly. Note that for $k = 1$ we obtain just the reduction criterion.

Theorem 2.2.3. *Let Λ_p be a linear map defined by*

$$\Lambda_p(X) = \text{Tr}(X)\mathbb{1} - pX, \tag{2.5}$$

be a linear map. Then Λ_p is k-positive for

$$\frac{1}{k + 1} \le p \le \frac{1}{k}, \tag{2.6}$$

but not $k + 1$-positive.

Next we give a characterisation of $\mathcal{S}_k$ in terms of positive maps, similar to Theorem 1.2.5. For the proof one needs the following lemma.

Lemma 2.2.3. *A linear map $\Lambda : \mathcal{L}_{\mathcal{H}_A} \to \mathcal{L}_{\mathcal{H}_B}$ is k-positive if and only if $\Lambda^\dagger : \mathcal{L}_{\mathcal{H}_B} \to \mathcal{L}_{\mathcal{H}_A}$ is k-positive.*

Proof. Suppose Λ is k-positive, then we have

$$\langle\psi|(\mathbb{1}_k \otimes \Lambda)(|\phi\rangle\langle\phi|)|\psi\rangle \ge 0,$$

where $|\phi\rangle \in \mathcal{H}_k \otimes \mathcal{H}_A$ and $|\psi\rangle \in \mathcal{H}_k \otimes \mathcal{H}_B$ are arbitrary and both have Schmidt rank k. Applying the definition of an adjoint map yields

$$\langle\phi|(\mathbb{1}_k \otimes \Lambda^\dagger)(|\psi\rangle\langle\psi|)|\phi\rangle \ge 0$$

for arbitrary $|\phi\rangle$ and $|\psi\rangle$ of Schmidt rank k.   □

Corollary 2.2.1. *A density operator ρ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ belongs to $\mathcal{S}_k$ if and only if*

$$(\mathbb{1} \otimes \Lambda)(\rho) \ge 0,$$

for all k-positive maps $\Lambda : \mathcal{L}_{\mathcal{H}_B} \to \mathcal{L}_{\mathcal{H}_A}$.

Proof. This follows from Theorem 2.2.2 and Corollary 2.1.1 in a completely analogous way as we derived Theorem 1.2.5. □

2.3   A conjecture

The detection of PPT entangled states is a difficult problem and this suggests that PPT entangled states have generically a low degree of entanglement. In particular we expect PPT entangled states to have a relative low Schmidt number. In Ref. [84, 257] evidence was given for the following conjecture.

Conjecture 2.3.1. *All entangled PPT states on $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^3$ have Schmidt number two.*

It is easy to see that this conjecture is equivalent to the statement that all 2-positive maps on $\mathcal{L}_{\mathbb{C}^3}$ are decomposable. A first piece of evidence is that the conjecture holds for PPT entangled states of rank 4 [257].

Lemma 2.3.1. *All entangled PPT states on $\mathcal{H} = \mathbb{C}^3 \otimes \mathbb{C}^3$ of rank four have Schmidt number two.*

Proof. Obviously it is sufficient to show this for edge states. So let ρ be a rank four edge state. We will show explicitly how to write ρ as a convex sum of Schmidt rank two vectors, by iterative subtracting of such vectors (in this context, see also Ref. [182]).

Since in $\mathbb{C}^3 \otimes \mathbb{C}^3$ there exists a UPB of 5 product states there must exist a product vector $|ef_1\rangle$ in the kernel of ρ. Since $\mathrm{Tr}(\rho|ef_1\rangle\langle ef_1|) = \mathrm{Tr}(\rho^{T_B}|ef_1^*\rangle\langle ef_1^*|) = 0$ and $\rho^{T_B} \geq 0$ we have that $|ef_1^*\rangle$ belongs to the kernel of ρ^{T_B}.

Constructing an orthogonal basis $\{|f_i\rangle\}$ we have that $\langle f_i^*|\rho^{T_B}|ef_1^*\rangle = 0 = \langle f_1|\rho|ef_i\rangle$, so that for instance for $i = 2$,

$$|\psi_1\rangle = \rho|ef_2\rangle = |cf_2\rangle + |df_3\rangle.$$

Since this vector has at most Schmidt rank two and belongs to the range of ρ, we can subtract it and obtain a new state

$$\tilde{\rho} = \rho - \Lambda|\psi_1\rangle\langle\psi_1|,$$

with

$$\frac{1}{\Lambda} = \langle\psi_1|\rho^{-1}|\psi_1\rangle = \langle\psi_1|ef_2\rangle.$$

The state $\tilde{\rho}$ has rank three and it is easy to verify that $\tilde{\rho}|ef_1\rangle = \tilde{\rho}|ef_2\rangle = 0$ but

$$|\psi_2\rangle = \tilde{\rho}|ef_3\rangle = |\tilde{c}f_2\rangle + |\tilde{d}f_3\rangle.$$

This vector has again at most a Schmidt rank two vector, and we can again subtract it to obtain

$$\tilde{\tilde{\rho}} = \tilde{\rho} - \tilde{\Lambda}|\psi_2\rangle\langle\psi_2|,$$

with

$$\frac{1}{\tilde{\Lambda}} = \langle\psi_2|\tilde{\rho}^{-1}|\psi_2\rangle = \langle\psi_2|ef_3\rangle.$$

The state $\tilde{\tilde{\rho}}$ has rank two and $\tilde{\tilde{\rho}}|ef_1\rangle = \tilde{\tilde{\rho}}|ef_2\rangle = \tilde{\tilde{\rho}}|ef_3\rangle = 0$. From this follows that we can write ρ as

$$\rho = \tilde{\tilde{\rho}} + \tilde{\Lambda}|\psi_2\rangle\langle\psi_2| + \Lambda|\psi_1\rangle\langle\psi_1|.$$

Since $\tilde{\tilde{\rho}}$ effectively acts on $\mathbb{C}^2 \otimes \mathbb{C}^3$ it has Schmidt number two and therefore ρ has also Schmidt number two. □

In order to check the conjecture for arbitrary rank, first note that again it is sufficient to check it for edge states. Let $\mathcal{W}$ denote the set of all entanglement witnesses detecting these edge states. Then the conjecture is equivalent to the statement that for all $W \in \mathcal{W}$ on $\mathbb{C}^3 \otimes \mathbb{C}^3$ there exists a Schmidt rank two vector $|\psi\rangle$ such that $\langle\psi|W|\psi\rangle < 0$. Now in $\mathbb{C}^3 \otimes \mathbb{C}^3$ the sum of the ranks of ρ and ρ^{T_B} are not larger than 13 for edge states [151, 176]. For states with such a relative low rank Sanpera et al. [257] gave an argument that such a $|\psi\rangle$ always exists (for a generalisation to higher dimensions, see Ref. [152]). Their argument is based on counting the degrees of freedom versus the number of constraints in constructing such a $|\psi\rangle$. Their argument is especially weak for ranks $(6,6)$ and $(8,5)$ since here only a finite number of solutions can be found, for which it is by no means guaranteed they will satisfy the constraints. When the conjecture was first published only PPT edge states of rank $(4,4)$ and $(6,7)$ were known. In view of the conjecture, there was special interest in constructing PPT edge states with ranks $(6,6)$ and $(8,5)$. In a recent paper Ha and Kye [113] managed to find edge PPTES

for all ranks except $(5,5)$ and $(6,6)$. It is for this reason we have specially constructed such states in Section 1.2.4.

For these states, we can construct witnesses in a number of different ways. First note that both states violate the realignment criterion, and thus using Theorem 1.3.4 we obtain W_1. Secondly, there is the canonical construction for edge states of Theorem 1.2.8, which gives us W_2. Thirdly, one can use the algorithm [75] from Section 1.2.5 yielding W_3. Numerically we calculated all three witnesses W_1, W_2 and W_3 for $\rho_{(5,5)}$ and $\rho_{(6,6)}$. After normalisation we found that all witnesses are different and yield a different value on the states. In total this gives us six different non-decomposable witnesses. We have checked that these witnesses are negative on some Schmidt rank two state. This provides additional evidence in favour of the conjecture. In fact, we also verified this for the witnesses

$$\tilde{W}_i = W_i - (\text{Tr}(W_i\rho) + \epsilon)\mathbb{1},$$

for arbitrarily small $\epsilon > 0$. These witnesses $\tilde{W}_i$ barely detect our states and are therefore the best candidates to check the conjecture. Note, however, that this is only evidence that the states have Schmidt number two. A full proof would consist of an explicit decomposition in Schmidt rank two states. However, finding such a decomposition is in general a very hard problem and we did not attempt this.

2.4   Schmidt robustness

In this section we generalise the notion of robustness of entanglement (see also Section 3.3) to the robustness of Schmidt number, which we analyse for pure states. We start by recalling the definition of robustness of entanglement [117, 274, 304].

The $\mathcal{K}$-*robustness* of a state ρ, $R_k(\rho) \geq 0$ is the minimal value of R such that

$$\frac{1}{1+R}(\rho + R\rho_k)$$

is separable, for some state $\rho_k \in \mathcal{K}$. Thus robustness measures measure how much mixing is required before a state becomes separable. With this basic definition we have

The robustness $R_s(\rho)$ Here $\mathcal{K} = \mathcal{S}$, the set of separable states.

The random robustness $R_r(\rho)$ Here $\mathcal{K} = \{\mathbb{1}\}$, the maximally mixed state)[1].

The generalised robustness $R_g(\rho)$ Here $\mathcal{K} = \mathcal{D}$, the set of all states.

From the definitions it is clear that $R_g \leq R_s \leq R_r$. Both the robustness and the generalised robustness are entanglement monotones (see Section 3.3). It is easy to see from the definition that the random robustness is proportional to the so-called witnessed entanglement [35], defined as $\max_{W \in M}[0, -\operatorname{Tr}(\rho W)]$ where M is the set of all normalised entanglement witnesses. The following theorem gives exact values for the robustness and the random robustness for pure states.

Theorem 2.4.1 ([117, 274, 304]). *Let* $|\psi\rangle = \sum_i a_i |ii\rangle$ *be a pure bipartite state with ordered Schmidt coefficients* $a_i \geq a_{i+1}$. *The robustness of* ψ *is given by*

$$R_s(\psi) = \sum_{i \neq j} a_i a_j = (\sum_i a_i)^2 - 1 = R_g(\psi)$$

and equals its generalised robustness.

A separable state that washes out the entanglement in ψ *most quickly is given by*

$$\rho_s = \rho_g = \frac{1}{R_s} \sum_{i \neq j} a_i a_j |ij\rangle\langle ij|.$$

The random robustness of ψ *is given by* $R_r(\psi) = a_1 a_2$.

An alternative proof of this theorem can be obtained as a corollary of our results (see Section 2.4.1). In what follows, we assume that all states act on a Hilbert space $\mathcal{H} \cong \mathbb{C}^d \otimes \mathbb{C}^d$. Throughout we also use local operations and classical communication (LOCC, see Chapter 3), as they do not increase the Schmidt number.

2.4.1 Generalised Schmidt robustness

In this section we will extend the notion of generalised robustness to generalised Schmidt robustness. Analogously to the generalised robustness, the generalised Schmidt-n robustness of a state ρ, $R_{gn}(\rho)$ is defined as the minimal value of R such that

$$\frac{1}{1+R}(\rho + R\rho_{gn})$$

---

[1]For simplicity we have chosen not to normalise $\mathbb{1}$ in the definition, in contrast to the original definition of random robustness in Ref. [304].

has Schmidt number smaller or equal than n, for some ρ_{gn}.

Let us now analyse the generalised Schmidt robustness for pure states. In Theorem 2.4.1 we have seen that for a pure state $|\psi\rangle = \sum_i a_i |ii\rangle$ the state

$$\rho_g = \frac{1}{R_g} \sum_{i \neq j} a_i a_j |ij\rangle\langle ij|, \tag{2.7}$$

erases most quickly the entanglement present in $|\psi\rangle$. It is plausible that this same state will also erase Schmidt number in an optimal way. We were able to prove this for the maximally entangled state. For the maximally entangled state $|\psi_+\rangle = \frac{1}{\sqrt{d}}\sum_i |ii\rangle$, ρ_g given by 2.7 reduces to $\rho_g = \frac{1}{d^2-d}(\mathbb{1} - Z)$, with $Z = \sum_i |ii\rangle\langle ii|$.

Theorem 2.4.2 (Generalised Schmidt robustness of the maximally entangled state). *The state defined by*

$$\rho(\beta) = \frac{\beta \rho_g + P_+}{1 + \beta} \quad where \quad \rho_g = \frac{\mathbb{1} - Z}{d^2 - d} \tag{2.8}$$

has Schmidt number n for

$$\frac{d - n}{n} \leq \beta < \frac{d - n + 1}{n - 1}.$$

The generalised Schmidt-n robustness of the maximally entangled state P_+ is given by

$$R_{gn}(P_+) = \frac{d - n}{n}.$$

Proof. Let $S(\beta)$ be the Schmidt number of $\rho(\beta)$ and let $\beta_n = \frac{d-n}{n}$. We first show that $S(\beta_n) \leq n$.

(i) We will give an explicit decomposition of the state $\rho(\beta_n)$ in terms of Schmidt rank n states. Equivalently, we show how one can construct this state locally with the aid of Schmidt rank n states. In what follows we will often omit normalisation. Let us take a maximally entangled n-level state

$$|\psi_S\rangle = \frac{1}{n} \sum_{i \in S}^{n} |ii\rangle,$$

where $S = \{i_1, \ldots, i_n\}$ is a subset of $\{1, \ldots, d\}$. We can construct such a state in $\binom{d}{n}$ possible ways, and clearly all these states have Schmidt number n. Now let us mix with equal weight the corresponding states $|\psi_S\rangle\langle\psi_S|$. Then for every i and j we will have

$\binom{d-1}{n-1}$ terms of the form $|ii\rangle\langle ii|$ and $\binom{d-2}{n-2}$ terms of the form $|ii\rangle\langle jj|$, $i \neq j$. Thus the resulting state will be proportional to

$$(d-1)Z + (n-1)\sum_{i \neq j}|ii\rangle\langle jj|.$$

Therefore we have proven that the state (see Ref. [59] for n=2)

$$K = Z + \frac{d(n-1)}{d-n}P_+$$

has Schmidt number at most n. It turns out that we can transform this state in the form (2.8) by applying a certain partial twirl operation. Consider the following twirl operation [131, 241, 309]

$$\int dU(U \otimes U^*)\rho(U \otimes U^*)^\dagger,$$

which maps any state ρ into one of the form $\mathbb{1} + \alpha P_+$ (an isotropic state). Here dU is the uniform probability distribution on the unitary group $U(d)$. Note that the twirl can be implemented locally, both parties need to implement only one random unitary. Remarkably, it has been shown [83][2] that the integral can be written as a finite sum (for qubits this was first shown in Ref. [21]). This will allow us to perform a partial twirl, just by considering a part of this finite sum.

In the first step we apply the unitary transformation $(T \otimes T^*)K(T \otimes T^*)^\dagger$, with

$$T = \frac{1}{\sqrt{d}}\sum_{j,k=0}^{d-1} e^{\frac{i2\pi jk}{d}}|j\rangle\langle k|,$$

which is just the quantum Fourier transform. Since T is unitary, it acts as the identity on P_+ [131], while it acts on Z as

$$(T \otimes T^*)Z(T \otimes T^*)^\dagger = \frac{1}{d^2}\sum_a \sum_{j,k,s,t} e^{\frac{i2\pi(j-t+k-s)a}{d}}|j\rangle\langle t| \otimes |s\rangle\langle k|.$$

The terms of the form $|jj\rangle\langle kk|$ for $s = j$ and $t = k$ will give a contribution P_+, while the $|ij\rangle\langle ij|$ for $i \neq j$ (for $j = t$ and $k = s$) will give a contribution of $(\mathbb{1} - Z)/d$, so that

$$K' = d(T \otimes T^*)K(T \otimes T^*)^\dagger = \mathbb{1} - Z + \frac{d(d-1)n}{d-n}P_+ + L,$$

---

[2]In Ref. [83] the finite decomposition of the $U \otimes U$ twirl was given, but a similar decomposition can be deduced from it for the $U \otimes U^*$ twirl.

where L are terms not of the form $|ii\rangle\langle jj|$ or $|ij\rangle\langle ij|$. Now these contributions can be easily removed by repeated application of the following mixing procedure

$$K'' = \frac{1}{2}(U \otimes U^*)K(U \otimes U^*)^\dagger + \frac{1}{2}K'.$$

First U is chosen to act as $U|k\rangle = e^{i\pi\delta_{kl}}|k\rangle$ for every $l = 0, \ldots, d-1$. This defines d mixing procedures. Next U is taken to act as $U|k\rangle = e^{i\pi\delta_{kl}/2}|k\rangle$ (another d mixing procedures). One can readily check [83] that these operations do not affect terms $|ii\rangle\langle jj|$ or $|ij\rangle\langle ij|$ but cancel out L completely.

Thus $S(\beta_n) \leq n$. Now for $\beta_n \leq \beta < \beta_{n-1}$, the state $\rho(\beta)$ is a convex combination of $\rho(\beta_n)$ and $\rho(\beta_{n-1})$ and therefore $S(\beta) \leq n$.

(ii) For the second part, we generalise the trick introduced in Ref. [117]. For any state σ, suppose t is a positive number such that $P_+ + t\sigma$ has Schmidt number n. The operators $W_n = \mathbb{1} - d/nP_+$ witness Schmidt number $n+1$ (see Example 2.1.1), so that we have

$$0 \leq \mathrm{Tr}\left[(\mathbb{1} - d/nP_+)(P_+ + t\sigma)\right]$$
$$= 1 + t - d/n\,\mathrm{Tr}\,[P_+] - d/n\,\mathrm{Tr}\,[P_+\sigma]$$
$$\leq -\frac{d-n}{n} + t.$$

since $\mathrm{Tr}\,P_+\sigma \geq 0$. Thus $t \geq \beta_n$, and for $\sigma = \rho_g$ it follows that $S(\beta) \geq n$ for $\beta_n \leq \beta < \beta_{n-1}$.

For general σ, it follows that $R_{gn} \geq \beta_n$, but $\rho(\beta_n) = P_+ + \beta_n\rho_g$ has Schmidt number n, so that $R_{gn}(P_+) = \beta_n$. $\square$

Note that the states (2.8) constitute one of the very few examples of non-trivial one parameter states for which the Schmidt number is known. To our knowledge, the only other example is that of the isotropic states, Example 2.1.1. This theorem allows us to present non-trivial bounds to the generalised Schmidt robustness of arbitrary pure states.

Corollary 2.4.1 (Lower and upper bounds for the generalised Schmidt robustness).
The generalised Schmidt-n robustness R_{gn} of a pure state $|\psi\rangle = \sum_i a_i|ii\rangle$ satisfies

$$\frac{1}{n}(\sum_i a_i)^2 - 1 \leq R_{gn} \leq R_g\frac{d-n}{(d-1)n},$$

with $R_g = \sum_{i \neq j} a_i a_j = (\sum_i a_i)^2 - 1$ *the generalised robustness of* ψ.

Proof. In Theorem 2.4.2 we have seen that $\rho = \frac{d-n}{n} \frac{1}{d^2-d}(\mathbb{1} - Z) + P_+$ has Schmidt number n. Performing the filtering operation $(A \otimes A)\rho(A \otimes A)^\dagger$ we hence obtain a state with Schmidt number at most n (this is because local filtering cannot increase the Schmidt number of a state [286]). If we take $A = \sum_k \sqrt{a_k}|k\rangle\langle k|$ we obtain that

$$|\psi\rangle\langle\psi| + R_g \frac{d-n}{(d-1)n}\rho_g$$

has Schmidt number n. Here $\rho_g = \frac{1}{R_g} \sum_{i \neq j} a_i a_j |ij\rangle\langle ij|$ as before. This gives the upper bound. The lower bound can be readily proven using exactly the same trick as in part (ii) of Theorem 2.4.2.   □

The lower and upper bound only coincide when ψ is the maximally entangled state or when $n = 1$. Note that the lower bound can be negative. The upper bound depends on the dimension of the Hilbert space in which the state is embedded, and hence will in general not match the value of the generalised Schmidt robustness.

2.4.2   Random Schmidt robustness

We define the random Schmidt-n robustness of a state ρ, $R_{rn}(\rho)$ as the minimum value of R such that

$$\frac{1}{1+R}(\rho + R\mathbb{1})$$

has Schmidt number n.

Upper bounds

As we have seen from Example 2.1.1 for $\rho = P_+$ we have $R_{rn} = (d-n)/[d(nd-1)]$. For general pure states a (weak) upper bound to the random Schmidt robustness can be obtained as follows. We know that

$$\Gamma_n = (d-n)\mathbb{1} + (nd-1)dP_+$$

has Schmidt number n. Local filtering $(A \otimes A)\Gamma_n(A \otimes A)^\dagger$ cannot increase the Schmidt number. So that with $A = \sum_k \sqrt{a_k}|k\rangle\langle k|$ we obtain

$$\Gamma'_n = (d-n)\rho_A \otimes \rho_A + (nd-1)|\psi\rangle\langle\psi|,$$

with ρ_A the reduced density operator of $|\psi\rangle\langle\psi|$, and because $\mathbb{1} - \rho_A \otimes \rho_A$ is a separable state we get as an upper bound for the random Schmidt robustness $R_{rn}(\psi) \leq (d - n)/(nd - 1)$. The following theorem presents a non-trivial upper bound.

Theorem 2.4.3 (Upper bound to the random Schmidt robustness). *The random Schmidt-n robustness R_{rn} of a pure state $|\psi\rangle = \sum_i a_i|ii\rangle$ satisfies*

$$R_{rn} \leq \frac{R_r(d - n)}{dn - 1},$$

with $R_r = a_1 a_2$ the random robustness of ψ.

Proof. In this proof, we work again with unnormalised states. Note that, if we add two unnormalised Schmidt number n states together we end up with a state of at most Schmidt number n. Equivalently, this can be shown by mixing the normalised states with different weights.

Analogously to the construction in Theorem 2.4.2, let us take a maximally entangled n-level state

$$|\psi\rangle_S = \frac{1}{n} \sum_{i \in S}^{n} a_i|ii\rangle,$$

where $S = \{i_1, \ldots, i_n\}$ is a subset of $\{1, \ldots, d\}$. Again, we can construct such a state in $\binom{d}{n}$ possible ways, and mixing the corresponding (unnormalised) states $|\psi_S\rangle\langle\psi_S|$ together, we end up with a state proportional to

$$\sum_i a_i^2|ii\rangle\langle ii| + \frac{(n - 1)}{d - n}|\psi\rangle\langle\psi|,$$

which has at most Schmidt number n. Now, in Corollary 2.4.1 we have seen that the state

$$\frac{(d - 1)n}{d - n}|\psi\rangle\langle\psi| + \sum_{i \neq j} a_i a_j|ij\rangle\langle ij|$$

has Schmidt number at most n. Adding these two states together we find that

$$\frac{dn - 1}{d - n}|\psi\rangle\langle\psi| + \sum_{i,j} a_i a_j|ij\rangle\langle ij|$$

has Schmidt number no more than n. Mixing this state with the separable state $\sum_{i,j}(a_1 a_2 - a_j a_j)|ij\rangle\langle ij|$, we obtain finally

$$\frac{dn - 1}{(d - n)a_1 a_2}|\psi\rangle\langle\psi| + \mathbb{1}.$$

$\square$

Conjecture 2.4.1 (Schmidt balls around the identity)**.** *Consider the unnormalized mixture*

$$\rho_\beta = \mathbb{1} + \beta\rho, \qquad with \qquad -1 \leq \beta \leq \infty, \tag{2.9}$$

with ρ an arbitrary normalized state acting on $\mathbb{C}^d \otimes \mathbb{C}^d$. The state ρ_β has Schmidt number at most k for all *d and ρ when*

$$\beta \leq 2(2k^2 - 1). \tag{2.10}$$

Note that it is a generalisation of the fact that $\mathbb{1} + 2\rho$ is separable for all normalised states ρ [304]. The conjectured value (2.10) can be obtained as follows. Starting from the identity, it is natural to assume that we can go fastest to a higher Schmidt number by mixing with some maximally entangled state. Taking $\rho = P_+^{d'}$ (the maximally entangled d'-level state) we have that $\beta \leq d'(kd' - 1)/(d' - k)$, which reaches its maximum for $d' = \sqrt{k^2 - 1} + k$ or for integer $d' = 2k$. Substituting this expression in the expression for β gives the upper bound from the conjecture. Thus it looks like, starting from the identity, we can get most quickly to a Schmidt number $k + 1$ state by mixing with the maximally entangled state in $2k \otimes 2k$. Upper bounds on the random Schmidt number two robustness are particularly useful as a distillability criterion can be deduced from it, which we will discuss in Section 4.2.

Lower bounds

Lower bounds on the random Schmidt robustness of a pure state ψ can be obtained from any Schmidt witness that detects ψ. Indeed, suppose W_{n+1} is a normalised Schmidt number $n + 1$ witness such that $\text{Tr}(|\psi\rangle\langle\psi|W_{n+1}) = -\alpha$, with $\alpha > 0$. Then it is easy to see that $R_{rn}(\psi) \geq \frac{\alpha}{d^2}$. It follows that

$$d^2 R_{rn}(\psi) = - \min_{\text{Tr } W_{n+1}=1} \text{Tr}(|\psi\rangle\langle\psi|W_{n+1}).$$

The question is now to determine this class of optimal Schmidt witnesses. We have conducted a large numerical test and have found a class which we conjecture to be optimal. The construction is the following:

Consider the Schmidt witnesses $W_{n+1} = \mathbb{1} - d/nP_+$ from Example 2.1.1. Performing the filtering operation $(A \otimes B)W_{n+1}(A \otimes B)^\dagger$ we obtain again a Schmidt number $n + 1$

witness. Let us consider the particular case where $A = B = \sum_k \sqrt{a_k}|k\rangle\langle k|$ diagonal and such that $\sum_i a_i^2 = 1$; we obtain

$$\tilde{W}_{n+1} = \frac{n\sum_{ij} a_i a_j |ij\rangle\langle ij| - \sum_{ij} a_i a_j |ii\rangle\langle jj|}{n(\sum_i a_i)^2 - 1}. \tag{2.11}$$

For a given pure state $|\psi\rangle = \sum_i b_i |ii\rangle$ we therefore conjecture:

Conjecture 2.4.2. *The random Schmidt robustness R_{rn} of a pure state $|\psi\rangle = \sum_i b_i|ii\rangle$ is given by*

$$d^2 R_{rn}(\psi) = -\min_{\mathrm{Tr}\,\tilde{W}_{n+1}=1} \mathrm{Tr}(|\psi\rangle\langle\psi|\tilde{W}_{n+1}) = -\min_{a_i} \frac{n\sum_i a_i^2 b_i^2 - (\sum_i a_i b_i)^2}{n(\sum_i a_i)^2 - 1}, \tag{2.12}$$

with $\sum_i a_i^2 = 1$.

One can solve the minimisation problem with Lagrange multipliers [280]. The solution is given by

$$\min_{\mathrm{Tr}\,\tilde{W}_{n+1}=1} \mathrm{Tr}(|\psi\rangle\langle\psi|\tilde{W}_{n+1}) = -\lambda_{\min},$$

where $\lambda_{\min}$ is the minimum eigenvalue of

$$\left(\mathbb{1} - \frac{nJ}{nd-1}\right)(nD - B),$$

with J the all-ones matrix, D the diagonal matrix with $D_{ii} = b_i^2$ and B the matrix with coefficients $B_{ij} = b_i b_j$.

A first step in proving this conjecture would be to show that the class of witnesses $(A \otimes B)W_{n+1}(A \otimes B)^\dagger$ with A, B arbitrary matrices, is no more powerful than the class of witnesses $(A \otimes A)W_{n+1}(A \otimes A)^\dagger$, with A diagonal. We have numerically verified this for $n = 2, 3$ and $d = 3, 4$. In Figure 2.1 we have illustrated the minimization of (2.12) for a particular set of pure states (see caption).

In conclusion, we have presented strong upper and lower bounds for the generalised and random Schmidt robustness for pure states. The problem of finding exact values is very hard, as in the end, one has to come up with an explicit convex decomposition in Schmidt rank n states on the one hand, and on the other with a construction of optimal Schmidt witnesses. We hope that our results may stimulate further work, especially in proving or disproving Conjecture 2.4.1.
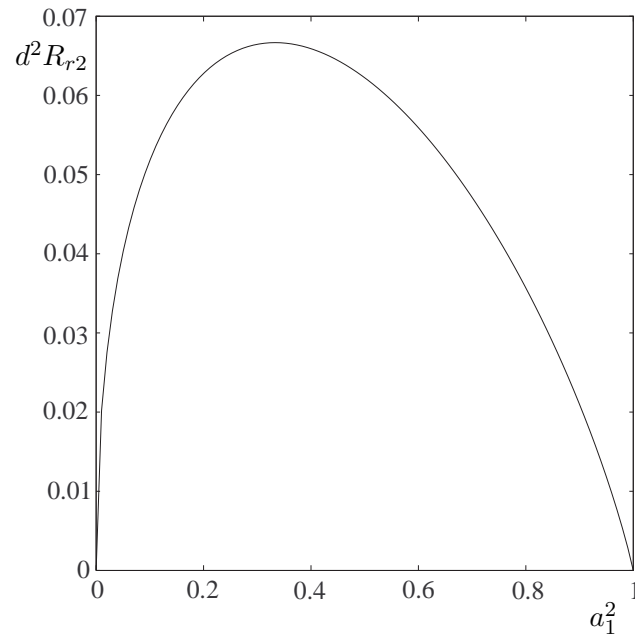
Figure 2.1: Lower bounds on $R_{r2}(\psi)$ as a function of a_1^2, where $|\psi\rangle = a_1|00\rangle + a_2(|11\rangle + |22\rangle)$. The graph was obtained using the witnesses from Conjecture 2.4.2.

Entanglement distillation: Introduction and classical results

Distillation is the process of converting with some finite probability a large number of mixed entangled states into a smaller number of maximally entangled pure states. It relies on local collective manipulation of the systems together with classical communication between the parties (LOCC). It has become apparent that characterizing and quantifying distillation is important in understanding the nature of entanglement from a physical point of view. Considerable effort has been devoted to the characterisation of distillable states, but even for bipartite systems the matter is not settled. In the next two chapters we analyse entanglement distillation in the bipartite scenario in great detail.

This chapter is meant as an introduction, and most of the material presented can be considered as literature review. In the first two chapters entanglement was studied as static material, however entanglement distillation involves manipulation of quantum states, so that we start this chapter with a study of quantum operations (Section 3.1). In the following section, this is then applied to the study of possible transformations between pure states both in the finite and asymptotic regime, with particular emphasis on entanglement concentration. In Section 3.3 we review the most important measures

of entanglement and some of their properties. These divide natural into two classes, the geometrical entanglement measures, such as robustness measures already encountered in the previous chapter, and operational measures. An example of the latter is the entanglement of distillation, which will be the main focus of our attention. We also show that in general, entanglement is not conserved in the asymptotic regime for mixed states. We discuss two examples of such irreversibility: the maximally correlated states and the bound entangled states. We end this chapter with a sketch of the most important distillation protocols for mixed states in the asymptotic regime.

3.1 Quantum operations

3.1.1 General quantum operations

A quantum operation Λ is a physical operation which transforms a state ρ on $\mathcal{H}_1$ into another state ρ' on $\mathcal{H}_2$. The aim of this section is to give a unified mathematical representation (the so-called Kraus formalism [77, 178, 215]) of any quantum operation, independent of how this operation is to be implemented physically. Basically, there are two approaches to this [138, 214]. The first is the axiomatic one: we impose on the class of maps $\Lambda : \mathcal{L}(\mathcal{H}_1) \rightarrow \mathcal{L}(\mathcal{H}_2)$ some physically motivated constraints and define the remaining operations as quantum operations. The second approach is constructive and the set of quantum operations is defined as the one which can be obtained by combining operations from a certain set of elementary operations. Both approaches turn out to be equivalent; we will sketch the proof of the equivalence here.

The standard quantum mechanical formalism allows us to carry out four elementary operations on quantum states:

(O1) Unitary transformations: $\rho \rightarrow U\rho U^\dagger$, with U a unitary operator.

(O2) Adding an uncorrelated ancilla: $\rho \rightarrow \rho \otimes \sigma$, with σ a density operator.

(O3) Tracing out part of the system: $\rho \rightarrow \mathrm{Tr}_{\mathcal{H}'}(\rho)$, with $\mathcal{H}_1 = \mathcal{H}' \otimes \mathcal{H}''$.

(O4) Projective measurements with possibly postselecting: $\rho \rightarrow \sum_{i=1}^{k} P_i \rho P_i$, with P_i, pairwise orthogonal projectors such that $\sum_{i=1}^{n} P_i = \mathbb{1}$ with $k \leq n$.

In general a quantum operation will only be successful with a certain probability $p = \text{Tr}(\Lambda(\rho))$, so that $\rho' = \Lambda(\rho)/p$, and Λ does not increase the trace. It is clear that the operations (O1)-(O3) can be represented as trace preserving completely positive (CP) maps. As the composition of CP maps is CP, we see that any quantum operation composed of operations (O1)-(O3) can be represented by a trace preserving completely positive map, these operations will also be called non-measuring operations. The reverse turns out to be true: any trace preserving completely positive map can be implemented by means of the quantum operations (O1)-(O3). This result follows from the Stinespring dilation theorem [77, 138, 174, 276]. Now we invoke the Choi representation of CP maps (in this context also called the Kraus representation), which says that any CP map Λ can be written as $\Lambda(\rho) = \sum_i L_i \rho L_i^\dagger$ for all $\rho \in \mathcal{L}(\mathcal{H}_1)$ (see Theorem 1.2.3). The operators L_i are commonly called the Kraus operators. For a trace preserving CP we have that $\sum_i L_i^\dagger L_i = \mathbb{1}$. If we allow operations of the type (O4), we have to relax this constraint to $\sum_i L_i^\dagger L_i \leq \mathbb{1}$ and renormalise the density operator after application of Λ. Another way is to keep the constraint $\sum_i L_i^\dagger L_i = \mathbb{1}$ but allow postselecting on the particular outcomes of i. Thus we obtain (see for instance Ref. [77]):

Theorem 3.1.1. *A quantum operation Λ can be decomposed into operations of the form (O1)-(O4) if and only if Λ acts as a completely positive trace non-increasing operator: $\Lambda(\rho) = \sum_i L_i \rho L_i^\dagger$, with $\sum_i L_i^\dagger L_i \leq \mathbb{1}$.*

From a physical point of view, the requirement that a quantum operation is CP and trace non-increasing, is obvious. Thus we could equally have started this section by demanding this, and we would also have arrived to the elementary operations (O1)-(O4).

3.1.2   Bipartite quantum operations

Consider now a bipartite system on $\mathcal{H}_A \otimes \mathcal{H}_B$. We will review some important classes of local quantum operations where increasing degrees of communication are allowed [22, 58, 77, 242].

$\diamondsuit$ **Local operations**. This is the class of operations generated by the operators which have Kraus operators of the form $A_i \otimes \mathbb{1}$ and $\mathbb{1} \otimes B_i$ with $\sum_i A_i^\dagger A_i = \sum_i B_i^\dagger B_i = \mathbb{1}$. In this restricted class of operations, the parties are not allowed to communicate and the

operations are non-measuring. Combining them yields for an arbitrary local operation $\Lambda(\rho) = \sum_{ij} (A_i \otimes B_j)\rho(A_i \otimes B_j)^\dagger$.

$\diamond$ **1-local operations**. Suppose we allow *local operations with one-way communication* from A to B. So let us suppose Alice performs a generalised measurement on her subsystem, with Kraus operators A_i with $\sum_i A_i^\dagger A_i = \mathbb{1}$. If the result of her operation is i the operation on the state acts as (notice that this is a trace decreasing operation as it will occur only with a certain probability)

$$\Lambda_i^A(\rho) = (A_i \otimes \mathbb{1})\rho(A_i^\dagger \otimes \mathbb{1}).$$

She will communicate Bob that she found result i, and depending on that outcome he will perform a certain trace preserving operation defined by B_{ji} operators, with $\sum_j B_{ji}^\dagger B_{ji} = \mathbb{1}$. Here the index i denotes that the operation Bob implements depends on the result that he got from Alice. Thus the state will change as

$$\Lambda_i^{AB}(\rho) = \sum_j (\mathbb{1} \otimes B_{ji})(A_i \otimes \mathbb{1})\rho(A_i^\dagger \otimes \mathbb{1})(\mathbb{1} \otimes B_{ji}^\dagger).$$

Now if this same procedure is done on many particles the total ensemble will change as

$$\Lambda^{AB}(\rho) = \sum_{ij} (A_i \otimes B_{ji})\rho(A_i^\dagger \otimes B_{ji}^\dagger).$$

Of course postselection (for certain i) can occur in one or more terms of this expression.

$\diamond$ **2-local operations**. This class is also known as the class of local operations with two-way classical communication (LOCC). This situation is somewhat more complicated, since in this case, it is useful to do alternating measurements and communications. Following a similar strategy as for 1-local operations, we focus on one particular outcome of each measurement, and do the summation at the end. Alice starts off with her measurements, and finds $i1$ as result, therefore the relevant operator is $A_{i1} \otimes \mathbb{1}$. She communicates her result to Bob and he will then perform $\mathbb{1} \otimes B_{j1}(i1)$ and communicate his result to Alice who will perform $A_{i2}(i1, j1) \otimes \mathbb{1}$. All these operators satisfy similar normalization properties as in the previous paragraph. In that way we get at the end of the series (for the total ensemble)

$$\Lambda(\rho) = \sum_m (A_m \otimes B_m)\rho(A_m \otimes B_m)^\dagger,$$

with $m = (i1, i2, \ldots, in, j1, j2, \ldots, jn)$ and

$$A_m = A_{in}(i1, i2, \ldots, i(n-1), j1, j2, \ldots, j(n-1)) \ldots A_{i2}(i1, j1) A_{i1},$$

$$B_m = B_{jn}(i1, i2, \ldots, in, j1, j2, \ldots, j(n-1)) \ldots B_{j2}(i1, i2, j1) B_{j1}(i1).$$

Here also, postselecting can be done for particular choices of $i1, \ldots, in, j1, \ldots, j(n-1)$.

$\diamond$ **Separable operations**. Separable operations are defined as any operation which can be written as

$$\Lambda(\rho) = \sum_i (A_i \otimes B_i) \rho (A_i \otimes B_i)^\dagger,$$

where each A_i and B_i are arbitrary operations (including measurements). The normalization condition is $\sum_i (A_i \otimes B_i)^\dagger (A_i \otimes B_i) = \mathbb{1}$. It is obvious that any LOCC is also separable, but the reverse is generally not true [22]. However, we do have the following theorem [58]:

Theorem 3.1.2. *It is* always *possible to simulate a separable operation using only LOCC, but with probability possibly smaller than 1.*

Proof. So, [57] suppose we have two sets of operators $\{A_i\}$ and $\{B_i\}$ such that $\sum_i (A_i \otimes B_i)^\dagger (A_i \otimes B_i) = \mathbb{1}$ and a state ρ. In general we will have that $\sum_i A_i^\dagger A_i \geq \mathbb{1}$ and $\sum_i B_i^\dagger B_i \geq \mathbb{1}$. We renormalise $A'_i = aA_i$ and $B'_i = aB_i$ so that $\sum_i A'^\dagger_i A'_i \leq \mathbb{1}$ and $\sum_i B'^\dagger_i B'_i \leq \mathbb{1}$. Then we let Alice and Bob perform the generalized measurements corresponding to these operators. They will obtain two measuring outcomes k_1 and k_2 and communicate their result to each other. Their strategy is to keep the state only if the outcomes of their measurement coincide, if $k_1 = k_2$. Forgetting which outcome was obtained, we see that ρ transforms as

$$\rho \to N \sum_i p_i \frac{(A'_i \otimes B'_i) \rho (A'_i \otimes B'_i)^\dagger}{p_i} = \sum_i (A_i \otimes B_i) \rho (A_i \otimes B_i)^\dagger, \qquad (3.1)$$

with $p_i = \text{Tr}[(A'_i \otimes B'_i) \rho (A'_i \otimes B'_i)^\dagger]$ and N an appropriate normalisation factor. $\qquad \square$

$\diamond$ **PPT preserving operations**. Literally, these are operations which map PPT states to PPT states. Or with Rains' definition [241] operations Λ such that the induced map

$$\tilde{\Lambda} : \rho \to \Lambda(\rho^{T_B})^{T_B}$$

is completely positive. All separable operations are PPT preserving, as follows from [138]

$$[(A \otimes B)\rho(A \otimes B)^\dagger]^{T_B} = [(A \otimes (B^\dagger)^T)\rho^{T_B}(A^\dagger \otimes B^T)].$$

PPT preserving operations are the first class of operations which can be regarded as non-local, as for instance creation of an entangled PPT state is a PPT preserving operation. The key result on PPT preserving operations is that they can be implemented using LOCC when both parties share a specific entangled PPT state. This was first realised in the seminal paper by Cirac et. al. [58]. They characterised completely general quantum operations (and in particular entangling operations) on bipartite systems by means of a generalised Jamiołkowski isomorphism. Because of its importance, we briefly sketch the isomorphism in the next section.

3.1.3   Entangling operations

The Jamiołkowski isomorphism (Section 1.2.2) is an isomorphism between a linear map from an input space to an output space and an operator defined over the tensor product of these two spaces. As we have illustrated, this correspondence is useful when the map acts on one part of a bipartite system. For maps acting on compound systems it is not so easy to interpret this duality. We now introduce an extension of the Jamiołkowski isomorphism with a very nice physical interpretation [58].

Suppose we have two systems A and B, each consisting of two d-level subsystems $A = A_1, A_2$ and $B = B_1, B_2$ respectively. We will establish an isomorphism between a CP map $\Lambda = \Lambda_{A_1 B_1} : \mathcal{L}(\mathcal{H}_{A_1 B_1}) \to \mathcal{L}(\mathcal{H}_{A_1 B_1})$ and an operator $D = D_{A_1 A_2, B_1 B_2}$ acting on the total system $\mathcal{H}_A \otimes \mathcal{H}_B$. The isomorphism is given by

$$D = \mathbb{1}_{A_2 B_2} \otimes \Lambda_{A_1 B_1}(P_{A_1 A_2} \otimes P_{B_1 B_2}), \tag{3.2}$$

where Λ is understood to act only on the systems A_1 and B_1. Here $P_{A_1 A_2}$ is the projector on the maximally entangled state $|\psi\rangle_{A_1 A_2} = \frac{1}{\sqrt{d}}|ii\rangle_{A_1 A_2}$ (and analogously for $P_{B_1 B_2}$). Equivalently we can write

$$\Lambda(\rho_{A_1 B_1}) = d^2 \operatorname{Tr}_{A_2 B_2}(D\rho^T_{A_2 B_2}) = d^4 \operatorname{Tr}_{A_2 A_3 B_2 B_3}(D\rho_{A_3 B_3} P_{A_2 A_3} P_{B_2 B_3}).$$

From (3.2) it follows that D is the result of the action of Λ on two systems A_1 and B_1 which are prepared in a maximally entangled state with two ancillary systems.

The second form has an equally simple interpretation: if both parties share a state D, then they can implement the map Λ on a certain state $\rho_{A_1 B_1}$ by simultaneous projecting $\rho_{A_3 B_3}$ and D on the maximally entangled states of $A_2 A_3$ and $B_2 B_3$. From this isomorphism one can easily deduce the following correspondences:

1. Λ is a separable operation if D is separable, and conversely Λ is an entangling operation if D is entangled (with respect to A and B).

2. Λ is a PPT preserving operation if and only if $D^{T_A} \geq 0$. Thus any PPT preserving operation can be implemented locally with the aid of a shared PPT state.

This isomorphism has a large number of applications (see the original reference and [81]) which would lead us too far to go into here. A simple application is the classification of global unitaries according to their entangling power on composite systems [314, 336, 337]. Entangling power of a unitary is defined as the average entanglement a unitary creates on product states. When Λ is a unitary map, D is a pure state and there exists a closed expression of the entangling power in terms of the entanglement of this state vector. Using this, we were able [64] to show that the unitaries with highest entangling power are special kinds of permutations, with possible exception for $d = 6$. The isomorphism then immediately yields a construction of generic examples of 4-qudit maximally entangled states for all dimensions except for 2 and 6.

3.2   Pure states and the reversibility of entanglement

In this section we will study the distillation of entanglement of *pure* bipartite quantum states, which is often referred to as entanglement concentration. An arbitrary pure state ψ can be represented by a vector $|\psi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B \cong \mathbb{C}^d \otimes \mathbb{C}^d$. Without loss of generality we have taken the dimensions of the two Hilbert spaces to be equal. A way of quantifying the entanglement of ψ is by looking at the local density operator $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. For a separable state $|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$, the reduced density operator equals $\rho_A = |\psi\rangle_A \langle\psi|$, and is thus a pure state. The reduced density operator of an entangled state will have a rank larger than one. If the reduced density matrix is proportional to the identity matrix the state is maximally entangled, as is the case for the EPR singlet. For such states there is no information available locally, although the

global state is known exactly [260, 295]. A way of quantifying the purity of a local density operator ρ_A is by calculating its von Neumann entropy $E(\psi) = -\text{Tr}(\rho_A \log_2 \rho_A)$. We will call this quantity the entropy of entanglement or simply the entanglement of ψ. Note that the entanglement is a fully additive measure: $E(\psi_1 \otimes \psi_2) = E(\psi_1) + E(\psi_2)$. Writing ψ in the Schmidt basis

$$|\psi\rangle = \sum_{i=1}^{d} \lambda_i |ii\rangle,$$

with $\lambda_i \geq \lambda_{i+1} \geq 0$ and $\sum_i \lambda_i^2 = 1$, the reduced density matrix can be written as $\rho_A = \sum_i \lambda_i^2 |i\rangle_A\langle i|$ and the entanglement of ψ as $E(\psi) = -\sum_i \lambda_i^2 \log_2 \lambda_i^2$. Maximally entangled states in a $d \otimes d$ system have Schmidt coefficients $\lambda_i = 1/\sqrt{d}$ and entanglement $E = \log_2 d$.

Entanglement concentration is the process of converting partially entangled states to maximally entangled states by LOCC. The reverse process is called entanglement dilution. We will show how in the asymptotic regime n arbitrary states ψ can be concentrated into $nE(\psi)$ singlets for $n \to \infty$. Conversely, $nE(\psi)$ singlets can be diluted into n states ψ for $n \to \infty$. From the above it follows that the entropy of entanglement quantifies entanglement of pure states in the most natural way since it is preserved in the asymptotic regime: a collection of n states ψ can be converted into m_n states ϕ with LOCC and the ratio m_n/n approaching $E(\psi)/E(\phi)$ for $n \to \infty$. The entanglement of a singlet is given by $E = 1$ and serves thus as a proper unit of entanglement, the so-called *ebit* [19].

In the first part of this section we discuss some elementary entanglement concentration protocols, and present a dilution protocol. Next, we list some celebrated theorems of general pure state transformation in the finite and asymptotic regime.

3.2.1   Pure state distillation protocols

Local filtering – the procrustean method

The procrustean[1] method is conceptually maybe the simplest entanglement concentration protocol [19]. It works even when both parties only share one single copy of the

---

[1]Procrustes is a giant from Greek mythology. Allegedly he would capture people and tie them to an iron bed. He would then hack off their legs or stretch them to make them fit the bed.

state. So let Alice and Bob share the state $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $\cos\theta \geq \sin\theta$, then we can define

$$A_0 = \frac{\sin\theta}{\cos\theta}|0\rangle\langle 0| + |1\rangle\langle 1|,$$
$$A_1 = \sqrt{\mathbb{1} - A_0^\dagger A_0}.$$

Now the protocol consists of Alice performing the measurement corresponding to these operators and communicating the result to Bob. The protocol will be successful when Alice obtains the outcome corresponding to A_0, in this case, occurring with probability $2\sin^2\theta$, the output state will be a maximally entangled singlet. This protocol is optimal for single qubits and we will later see an extension of this protocol which is optimal for any pure bipartite state. Such a one-sided generalised measurement, where the state is conditionally kept will be called filtering. This is a technique which will be useful for mixed states as well.

An analogous protocol works for entanglement dilution: if Alice and Bob start out with a maximally entangled singlet and Alice applies the operation defined by

$$A_0 = \cos\theta|0\rangle\langle 0| + \sin\theta|1\rangle\langle 1|,$$
$$A_1 = \sin\theta|0\rangle\langle 0| + \cos\theta|1\rangle\langle 1|,$$

then they obtain the state $|\psi\rangle$ with probability one.

Schmidt projection

Following [19] we illustrate this method for qubits. As the method does not work for one copy we suppose that Alice and Bob share n copies of the state $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$, so that the combined system is described by the state vector

$$|\Psi\rangle = |\psi\rangle^{\otimes n} = \otimes_{i=1}^{n}[\cos\theta|00\rangle_i + \sin\theta|11\rangle_i].$$

The binomial expansion of this will have 2^n terms of which $n + 1$ will have different coefficients and the $n + 1$ corresponding subspaces will be orthogonal. Let us label these subspaces by $k = 0, \cdots, n$ corresponding to the power in which $\sin\theta$ appears. Now Alice can perform a von Neumann measurement corresponding to these subspaces. The probability of projecting upon the k-th subspace is given by

$$p_k = \binom{n}{k}\cos^{2(n-k)}\theta\sin^{2k}\theta.$$

She can then communicate her result of the measurement to Bob or Bob can perform a similar measurement (which will have the same outcome). In either case they will end up with a maximally entangled state in a known $2\binom{n}{k}$-dimensional space. After distilling many such states, they can be converted to singlets without loss of entanglement. In the asymptotic regime this protocol can be shown to be optimal: the ratio of singlets that can be distilled per input state ψ approaches $E(\psi)$ for the number of input states going to infinity. To achieve this, the Schmidt projection protocol has to be applied N times on batches of n states, with both N and n going to infinity.

Entanglement swapping

The phenomenon of entanglement swapping [334, 338] was first studied in the context of coincidence count rates of entangled pairs of photons. In the experimental setup, two different sources emit pairs of entangled photons and two halves of the pairs are being measured simultaneously. The remaining halves then become entangled. Thus entanglement swapping is the phenomenon of two particles getting entangled without direct interaction (see Ref. [220] for an experiment demonstrating this effect). This phenomenon also occurs in a multipartite setting [29, 335], but has to our knowledge only been demonstrated for qubits.

The idea of using entanglement swapping as an entanglement concentration procedure was first introduced in Ref. [30]. Consider the following two states of photons

$$|\phi\rangle_{12} = \cos\theta|00\rangle + \sin\theta|11\rangle,$$
$$|\phi\rangle_{34} = \cos\theta|00\rangle + \sin\theta|11\rangle.$$

Suppose $|\phi\rangle_{12}$ is shared by both parties Alice and Bob, and in addition Bob has the state $|\phi\rangle_{34}$. When Bob measures particles 2 and 3 in the Bell basis $\{|00\rangle + |11\rangle, |00\rangle - |11\rangle, |01\rangle + |10\rangle, |01\rangle - |10\rangle\}$, the resulting state for particles 1 and 4 will be one of the four states

$$|\phi^{\pm}\rangle_{14} = \frac{1}{\sqrt{\cos^4\theta + \sin^4\theta}}(\cos^2\theta|00\rangle \pm \sin^2\theta|11\rangle),$$
$$|\psi^{\pm}\rangle_{14} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle),$$

the first two occurring with probability $(\cos^4\theta + \sin^4\theta)/2$ and the last two with probability $\sin^2\theta\cos^2\theta$. In the first two cases, the entanglement is lower than in the original pair, but in the last two cases Alice and Bob end up with a maximally entangled state. In any case, however, the procedure can be repeated. Repeating the whole protocol over and over again, yields on one hand a group of maximally entangled pairs, and on the other, completely separable states. The fraction of maximally entangled pairs achievable in this way turns out to be $2\cos^2\theta$. This number just equals the maximal probability of the initial state to be converted into a maximally entangled state. In this sense, the entanglement swapping protocol is optimal. Note that since the second pair belongs to Bob, he has complete control over it, and he could in principal use any two-qubit state. It turns out that when he uses a state which is less entangled, the protocol does not concentrate entanglement but destroys it. When the state he uses is more entangled, no entanglement is destroyed, but the concentration is less efficient. (Here the entanglement is measured as the amount of singlets distillable from the state). Extensions of this protocol have been proposed in Ref. [158, 264] which do not rely on such an iterative procedure since the second step of their protocol is just the procrustean method.

With this we conclude our discussion of elementary pure state entanglement concentration protocols. Various other protocols have been proposed, as for instance in Ref. [13]. Noteworthy is the protocol outlined in Ref. [221] which demonstrates that entanglement concentration is possible using the effects of quantum statistics of indistinguishable particles only.

3.2.2 Finite regime

In this section we will discuss the more general question of feasibility of arbitrary transformations between pure states. The first work on this subject was done by Lo and Popescu [190], in particularly they proved the following:

Theorem 3.2.1. *The Schmidt number of a pure bipartite state cannot increase under local quantum operations and classical communication. Entanglement manipulations of pure bipartite states with only one way communication are as powerful as those with two way communication, but they are more powerful than those with no communication. In*

other words, we can replace any LOCC protocol on pure states, no matter how complex, by a single local generalised measurement.

The groundbreaking work on pure state entanglement transformation was carried out by Vidal in Ref. [299], where he introduced the notion of an entanglement monotone. His work was significantly extended by several authors in a series of papers [116, 169, 170, 213, 301, 306]. Recently it became apparent that their proofs can be simplified by making use of the quantum steering theorem as recognized by Verstraete [295] to which we refer the reader for full proofs. An entanglement monotone μ is defined as a quantity associated with a quantum state which on average does not increase under local transformations. That is, if an LOCC maps a state ρ with probability p_i into states ρ_i then $\mu(\rho) \geq \sum_i p_i \mu(\rho_i)$. The following theorem by Vidal [299] is crucial:

Theorem 3.2.2. *The restriction of an entanglement monotone μ to pure states ψ is given by a unitarily invariant concave function of the local density operator $\mu(|\psi\rangle) = f(\rho^B)$.*

This theorem implies that any entanglement monotone acting on pure states

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}|ii\rangle$$

can be expressed as a concave function of its Schmidt coefficients[2] λ_i. An important class of entanglement monotones E_k, for $k = 2, \ldots, n$ is given by

$$E_k(\psi) = \sum_{i=k}^{d} \lambda_i = 1 - \sum_{i=1}^{k-1} \lambda_i,$$

where as usual $\lambda_i \geq \lambda_{i+1}$. The concavity of this function can be proven using the variational characterization of eigenvalues of a Hermitian matrix [126].

Clearly we have that if we can convert ϕ to ψ with certainty then we need to have $E(\psi) \leq E(\phi)$ for every entanglement monotone E, and in particular this has to be the case for $E = E_k$. A surprising result by Nielsen [213] is that the converse is true:

Theorem 3.2.3. *A necessary and sufficient condition for the transformation ϕ to ψ to be possible with certainty is that $E_k(\psi) \leq E_k(\phi)$ for $k = 2, \ldots, n$. Alternatively, in*

---

[2]For convenience Schmidt coefficients in this section denote the 'normal' Schmidt coefficients squared.

terms of majorization, this can be expressed as $\lambda_\psi \succeq \lambda_\phi$, where λ_ψ stands for the vector consisting of the Schmidt coefficients of ψ in decreasing order.

For anyone who is familiar with unitarily invariant norms, this result will be reminiscent of Ky Fan's dominance theorem for unitarily invariant norms and the dual representation in terms of symmetric gauge functions [25, 127]. In fact, something much stronger can be proven [116, 169, 301]:

Theorem 3.2.4. *The probabilistic transformation from a pure bipartite state ϕ into the ensemble $\{p_i, \psi_i\}$ can be accomplished using LOCC if and only if $p_i \vec{\lambda}_{\psi_i} \succeq \vec{\lambda}_\phi$ or equivalently $\sum_i p_i E_k(\psi_i) \leq E_k(\phi)$ for all k.*

Note that from the theorem follows that the maximum probability p of transforming ϕ into ψ can be written as $p = \min_k \frac{E_k(\phi)}{E_k(\psi)}$ or $p\vec{\lambda}_\psi \succeq \vec{\lambda}_\phi$. The non-trivial part of these theorems is to show that there is an actual protocol achieving the transformation. The reader is referred to [295] for an elementary proof. It is there shown how the protocol achieving the transformation can be built from a few simple generalised measurements.

Let us now return to entanglement concentration. The above theorem gives us the optimal probability of converting a pure state to a maximally entangled state of arbitrary dimension. When we allow the concentration of entanglement into different maximally entangled states (of different dimensions), we can ask how much entanglement can be distilled on average. This is answered in the following theorem [116, 169]:

Theorem 3.2.5. *The optimal entanglement concentration procedure for a single pure bipartite state ψ with Schmidt coefficients $\lambda_1 \geq \ldots \geq \lambda_d \geq 0$ is one that produces a maximally entangled state ϕ_j of $j \leq d$ levels with probability $p_j = j(\lambda_j - \lambda_{j+1})$. The corresponding optimal average distilled entanglement is*

$$\langle E \rangle_{max} = \sum_{k=1}^{d} (\lambda_j - \lambda_{j+1}) j \log_2 j.$$

The proof of this theorem uses techniques from linear optimization, showing that there exist optimal p_j compatible with Theorem 3.2.4. The protocol achieving these probabilities can be obtained by going through the proof of this theorem. However, in view of Theorem 3.2.1 there exists a single local generalised measurement which does

the job. The measurement operators corresponding to Alice's generalised measurement are

$$A_j = \sum_{i=1}^{j} \sqrt{\frac{\lambda_j - \lambda_{j+1}}{\lambda_i}} |i\rangle_A \langle i|, \tag{3.3}$$

$$\tag{3.4}$$

indeed it is easy to verify that $\sum_{j=1}^{d} A_j^\dagger A_j \leq \mathbb{1}$ and

$$A_j \otimes \mathbb{1} |\psi\rangle = \sqrt{p_j} |\phi_j\rangle. \tag{3.5}$$

This protocol, a generalised procrustean method, thus turns out to be optimal.

Another application of Theorem 3.2.4 is the idea of catalysis [170, 290], where a pure state is used to help converting one state into an other, such that the pure state is recovered at the end of the procedure. Mathematically this means that there exist states ϕ, ψ and χ such that

$$\lambda_\psi \not\succeq \lambda_\phi \qquad \text{but} \qquad \lambda_{\psi \otimes \chi} \succeq \lambda_{\phi \otimes \chi}.$$

Finally note that one can broaden the discussion about pure state transformations by including questions about the approximate transformation of one state into another, see Ref. [306].

3.2.3   Asymptotic regime

In the introduction we have already sketched the main result in the asymptotic regime, which we now state formally [19, 78, 236]:

Theorem 3.2.6. *In the asymptotic regime n arbitrary states ψ can be concentrated into $nE(\psi)$ singlets for $n \to \infty$. Conversely, $nE(\psi)$ singlets can be diluted into n states ψ for $n \to \infty$. Thus the entropy of entanglement is conserved in the asymptotic regime and hence quantifies entanglement of pure states in a unique way.*

One can prove the distillation rate using Theorem 3.2.5 [169], or using the Schmidt projection distillation protocol [19]. The dilution rate can be proved using the teleportation idea [19]. Both the dilution and distillation rate can also be proven using

Nielsen's theorem (Theorem 3.2.3). The crucial part of the latter exploits the asymptotic equipartition theorem which implies that $|\psi\rangle^{\otimes n}$ can be approximated by $2^{nE(\psi)}$ terms in the Schmidt decomposition.

In Ref. [191] Lo and Popescu showed that pure state entanglement is a truly interconvertible, in the sense that the amount of classical communication needed in the asymptotic regime vanishes. This is trivial for the entanglement concentration, as the Schmidt projection method works without communication. The dilution step is the nontrivial part, and it can be shown that $nE(\psi)$ singlets can be diluted into n pairs ψ with $\mathcal{O}(\sqrt{n})$ classical bits of communication. Recently other asymptotically optimal protocols have been proposed, some of which are universal[3] (see for instance [119, 205]).

The entanglement concentration protocols we studied in the previous subsection are all of probabilistic nature, with the notable exception of Nielsen's result. As a result, the protocols reaching the entanglement yield $E(\psi)$ in the asymptotic limit are all probabilistic in a finite number of copies and only become deterministic in the asymptotic limit. The following theorem gives an upper bound to the asymptotic yield of singlets we can distill from a pure state ψ if we only use protocols that are deterministic for any given number of copies [211, 212].

Theorem 3.2.7. *Let ψ be a pure state with Schmidt decomposition $|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}|ii\rangle$, then the maximum number of singlets that can deterministically be concentrated is given by $E_{det}(\psi) = -\log_2 \lambda_1$. When ψ is a two-qubit state this bound can be obtained by a series of two-pair manipulations.*

Note that E_{det} just like E is a fully additive measure. The upper bound follows from Nielsen's theorem. The surprising result here is the situation for qubits where two-pair manipulations are sufficient. This is in sharp contrast with the probabilistic concentration protocols which generally need to be applied on a very large number of pairs. The values of E_{det} and E do not coincide, although both yields can be reached with probability one in the asymptotic limit. One can generalise this and ask for the distillable entanglement as a function of an error exponent, representing the rate of decrease in failure probability as the number of copies tends to infinity [118, 120].

---

[3]Sometimes also called blind protocols as neither prior knowledge of the state nor any form of quantum tomography is required.

3.3   Mixed states and the irreversibility of entanglement

As we have seen in the previous section, for pure states there are essentially a finite number of entanglement measures in the finite regime and a unique measure in the asymptotic regime. There are two obvious ways of quantifying mixed state entanglement, operational and geometrical. Operational entanglement measures are directly related to the physical applicability of entanglement. Geometrical measures can loosely be described as those quantifying the distance from a state to the set of separable states. As excellent reviews [54, 130, 230] have appeared recently in the literature, we do not attempt to give an extensive review of the subject here. In particular the geometrical entanglement measures will be treated in brief, while for the operational measures we focus mainly on the entanglement of distillation. For simplicity, entanglement measures here are defined simply as entanglement monotones and thus all presented measures vanish on separable states and are on average non-increasing under LOCC, unless otherwise stated.

3.3.1   Geometric measures

The first rigorous study of entanglement measures based on distance was carried out in Ref. [293, 294]. Intuitively, the quantity

$$\min_{\sigma \in \mathcal{S}} D(\rho || \sigma),$$

with D a suitable distance measure, can be regarded as a measure of entanglement. The most important measure of this kind arises when D is the quantum relative entropy $D = S(\rho || \sigma) = \text{Tr}(\rho \log_2 \rho - \rho \log_2 \sigma)$ [255, 261, 291]. The associated measure will be called the relative entropy of entanglement and denoted E_R. Note that for pure states, E_R reduces to the entropy of entanglement E. Although the relative entropy of entanglement is a distance measure, it stretches much further as it has several operational interpretations (see also next section).

A related measure [293] can be defined by using as a distance measure the Hilbert-Schmidt distance $D = ||\rho - \sigma||_2$. Although this quantity has received considerable interest, it was shown not to be an entanglement monotone [219]. We will call this measure the best separable approximation in the Hilbert-Schmidt norm analogous to

the best separable approximation BSA(ρ) in the trace norm [182], which can be shown to be a proper measure of entanglement. It is defined as

$$\text{BSA}(\rho) = \min\{\|\rho - \rho_{\text{s}}\| \,|\, \rho \geq \rho_{\text{s}}, \rho_{\text{s}} \in \mathcal{S}\}.$$

or equivalently

$$\text{BSA}(\rho) = \min\{\lambda | \rho = (1 - \lambda)\rho_{\text{s}} + \lambda\rho_{\text{e}}, \rho_{\text{s}} \in \mathcal{S}, \rho_{\text{e}} \in \mathcal{D} \setminus \mathcal{S}\}.$$

The geometric measure of entanglement (GME) is historically the first example of an entanglement measure. It was originally introduced by Shimony in Ref. [266] for pure states only as

$$\text{GME}(\psi) = \frac{1}{2}\min\{\| \,|\psi\rangle - |\phi\rangle| \,\|^2, \phi \in \mathcal{S}\} = 1 - \max\{|\langle\phi|\psi\rangle|^2 | \,\phi \in \mathcal{S}\}.$$

Thus the GME is proportional to the maximum overlap with a separable state. This measure was extensively analysed in Ref. [317], including for multipartite and mixed states. The mixed state generalisation of the GME was done by the usual convex roof construction, that is as a minimisation over all convex expansions of ρ:

$$\text{GME}(\rho) = \min\left\{\sum_i p_i \text{GME}(\psi_i) \middle| \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, p_i \geq 0\right\}.$$

Dual to the distance measures are the robustness measures. While distance measures quantify the distance of a set to the set of separable states, robustness measures quantify to which extend entangled states remain entangled under mixing. Recall (Section 2.4) that the robustness R_k relative to a set $\mathcal{K}$ is defined as

$$R_k(\rho) = \min\left\{R\middle|\frac{\rho + R\rho_k}{1 + R} \in \mathcal{S}, \rho_k \in \mathcal{K}, R \geq 0\right\}.$$

Taking $\mathcal{K}$ to be either $\mathcal{S}$, $\{\mathbb{1}\}$ or $\mathcal{D}$ we obtain respectively the robustness R_s, the random robustness R_r and the generalised robustness R_g. Note that the random robustness R_r was shown not to be an entanglement monotone [117]. However, for a given dimension, the maximum random robustness over all entangled states gives rise to a lower bound on the volume of separable states [304].

All the previous entanglement measures are very hard to evaluate for a general mixed state. For a NPT entangled state ρ, one can envisage that the sum of the negative

Measure	Definition	Key references
Relative entropy	$\min\{\mathrm{Tr}(\rho\log_2\frac{\rho}{\sigma})|\sigma\in\mathcal{S}\}$	[123, 231, 293, 294, 309]
BSA in trace norm	$\min\{\|\rho-\rho_{\mathrm{s}}\|\,|\rho\geq\rho_{\mathrm{s}},\rho_{\mathrm{s}}\in\mathcal{S}\}$	[151, 171, 182, 193, 320]
BSA in HS-norm	$\min\{\|\rho-\rho_{\mathrm{s}}\|_2|\rho_{\mathrm{s}}\in\mathcal{S}\}$	[24, 192, 219, 293, 323]
Robustness	$\min\{R\geq 0|\rho+R\rho_s\in\mathcal{S},\rho_s\in\mathcal{S}\}$	[117, 304]
Gen. robustness	$\min\{R\geq 0|\rho+R\rho_d\in\mathcal{S},\rho_d\in\mathcal{D}\}$	[34, 41, 117, 274]
Ran. robustness	$\min\{R\geq 0|\rho+R\mathbb{1}\in\mathcal{S}\}$	[32, 117, 304]
GME (pure)	$1-\max\{|\langle\phi|\psi\rangle|^2|\,\phi\in\mathcal{S}\}$	[31, 41, 266, 317, 318, 319]
Log. negativity	$\log_2\|\rho^{T_B}\|$	[229, 305]

Table 3.1: Geometrical measures of entanglement.

eigenvalues, the so-called negativity $\mathcal{N}(\rho)$, quantifies to some extent the distance of ρ to the set of PPT states [342]. And indeed, it can be shown to be an entanglement monotone. However, it is often more convenient to work with the logarithmic negativity [305], defined as

$$E_N(\rho)=\log_2\|\rho^{T_B}\|.$$

The reason is that E_N is fully additive by construction and also has considerable operational meaning, some of which we will outline in the next section (see also [9]).

With this, we conclude our roller coaster through the main geometric entanglement measures. Note that they also can be approached in a more unified way using either base norm Ref. [230, 309] or entanglement witnesses Ref. [33].

3.3.2   Operational measures

Having a unique measure for pure states in the asymptotic regime, it would be natural to ask if one can generalise this to mixed states. We have seen that for pure states, this measure quantifies both the amount of entanglement that can be distilled from them in the asymptotic regime and the amount of entanglement needed to construct the state in the asymptotic regime. Initially, the idea was to define two different measures for these quantities for mixed state: the distillable entanglement E_D and the entanglement cost E_C respectively.

A first attempt to the entanglement cost was made in Ref. [21] as the convex roof of the entanglement

$$E_F(\rho) = \min \sum_i p_i E(|\psi_i\rangle)$$

where the minimum is taken over all convex decomposition $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. This quantity is now known as the entanglement of formation. The evaluation of E_F for a general mixed state is very hard, and analytical results are only known for high symmetric states [287, 309] (see also [46] and reference therein). The notable exception is for 2 qubit systems, where an exact analytic formula is known in terms of the concurrence [326, 327].

It is however not clear that E_F has the operational meaning we want it to have [122]. In particular $E_F(\rho)$ quantifies the entanglement needed to construct ρ via *a specific procedure*. Namely, given a decomposition $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, one chooses with probability p_i a particular $|\psi_i\rangle$. Then, one constructs ψ_i out of singlets (costing in the asymptotic regime $E(\psi_i)$ ebits) and forgets the particular ψ_i chosen. In this way, we obtain one copy of ρ. Repeating this process over and over, then to construct ρ on average we need $E_F(\rho)$ ebits. Other procedures might be more efficient, such as constructing more than one copy at the time. In particular it is easy to see that

$$E_F^\infty(\rho) = \lim_{n\to\infty} \frac{E_F(\rho^{\otimes n})}{n} \leq E_F(\rho).$$

This quantity $E_F^\infty(\rho)$ is known as the regularised entanglement of formation.

In Ref. [122] it was rigorously proven that $E_F^\infty(\rho)$ equals the asymptotic value of m/n such that m qubits can be converted into n copies of ρ. This asymptotic yield, we call the entanglement cost and is formally defined as (see Ref. [230])

$$E_C(\rho) = \inf \left\{ r \,\bigg|\, \lim_{n\to\infty} \Big[\inf_\Lambda \|\Lambda(P_+^{\otimes nr}) - \rho^{\otimes n}\|\Big] = 0 \right\}$$

where the second infimum is taken over all trace preserving LOCC Λ and P_+ is the maximally entangled singlet state. We have used the trace norm in this definition, but some other measures work as well. Note that the equivalence $E_F^\infty(\rho) = E_C(\rho)$ is highly non-trivial as E_F^∞ gives rise to a protocol with a variable number of input singlets, while E_C works with a fixed number of input singlets. Now even more surprising, it is conjectured that the entanglement of formation is additive, in which case we would have

$E_C = E_F$. This additivity is one of the major open problems in quantum information theory (see Ref. [10, 207, 268] and references therein). Calculating the entanglement cost is very hard problem, and its value is only known so far in cases where one can prove the additivity [140, 206, 207, 265, 307, 333]. Both the entanglement of formation and the entanglement cost can be proven to be convex [78].

We now move on to the entanglement of distillation [21, 241, 242], quantifying how much pure state entanglement we can extract from a state ρ. Analogously to the entanglement cost we define

$$E_D(\rho) = \sup\left\{r \,\middle|\, \lim_{n\to\infty}\left[\inf_\Lambda \|P_+^{\otimes nr} - \Lambda(\rho^{\otimes n})\|\right] = 0\right\} \tag{3.6}$$

where the second supremum is taken over all trace preserving LOCC Λ and P_+ is the maximally entangled singlet state. Note that just like in the definition of E_C, the maximisation is over all protocols where the output has a fixed number of singlets. But similar to the entanglement cost, it has been proven rigorously [242] that allowing stochastic protocols does give rise to the same value for E_D. To elaborate a bit more on this point, suppose we have a protocol that from k copies of a state ρ produces n singlets for half of the time and no singlets at all for the other half. However, the above definition only allows deterministic protocols, that is in our case we would like to replace this stochastic protocol by a deterministic protocol which produces exactly $n/2$ singlets. The equivalence of both definitions says that in the asymptotic regime this can always be done. The proof of the equivalence exploits the law of large numbers, as when a stochastic protocol is repeated a large number of times, it can be approximated with a deterministic protocol on a larger input.

From the above, it will be clear that $E_D \leq E_C$. The following theorem [78, 135] pushes this observation further, stating that under some reasonable conditions the entanglement cost and the entanglement of distillation are extremal measures.

Theorem 3.3.1. *Let E be a positive functional on the set of states $\mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ satisfying for all states $\rho \in \mathcal{D}$*

1. *Normalisation: For any d-level maximally entangled state P_+^d, $E(P_+^d) = \log_2 d$.*

2. *Weak LOCC monotonicity: For any trace preserving LOCC map Λ: $E(\rho) \geq E(\Lambda(\rho))$.*

3. *Continuity: Let $(\rho_n)_{n\in\mathbb{N}}$ and $(\sigma_n)_{n\in\mathbb{N}}$ be any two sequences of states on $(\mathcal{H}_n^A)_{n\in\mathbb{N}}$ and $(\mathcal{H}_n^B)_{n\in\mathbb{N}}$ respectively. If $\|\rho_n - \sigma_n\| \to 0$ then*

$$\frac{E(\rho_n) - E(\sigma_n)}{1 + \log_2 \dim \mathcal{H}_n} \to 0$$

Then:

(i) If E is additive ($E(\rho^{\otimes n}) = nE(\rho)$ for all $\rho \in \mathcal{D}$) then

$$E_D(\rho) \leq E(\rho) \leq E_C(\rho).$$

(ii) If the regularisation $E^\infty(\rho) = \lim_{n\to\infty} E(\rho^{\otimes n})/n$ exists for all $\rho \in \mathcal{D}$ then

$$E_D(\rho) \leq E^\infty(\rho) \leq E_C(\rho).$$

In some sense this theorem is a weakened version of the asymptotic reversibility for pure states. The above theorem can be used to provide both lower bounds to the entanglement cost and upper bounds to the entanglement of distillation. The conditions for the latter can be slightly relaxed [135].

Theorem 3.3.2. *Let E be a positive functional on the set of states $\mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ satisfying for all states $\rho \in \mathcal{D}$*

1. *Weak LOCC monotonicity: For any trace preserving LOCC map Λ: $E(\rho) \geq E(\Lambda(\rho))$.*

2. *Partial sub-additivity: $E(\rho^{\otimes n}) \leq nE(\rho)$.*

3. *Continuity for the isotropic state (2.1)*

$$\rho(\beta_d, d) = \frac{1}{d^2 + \beta_d}(\mathbb{1} + \beta_d P_+).$$

That is, if we have a sequence of isotropic states $(\rho(\beta_d, d))_d \to P_+$ when $d \to \infty$, then we require that

$$\lim_{d\to\infty} \frac{E(\rho(\beta_d, d))}{\log_2 d} \to 1.$$

Then $E_D(\rho) \leq E(\rho)$ for all ρ.

Thus for an entanglement measure to be an upper bound to the entanglement of distillation it is enough to be continuous in the neighborhood of the maximally entangled state. We proceed by giving some examples of entanglement measures that are strictly larger than E_D. The relative entropy of entanglement E_R was the first example of an upper bound to E_D [135, 241, 293, 294], this follows relatively easily from the previous theorem. Another early upper bound to E_D is given by the logarithmic negativity E_N [305], and again one easily verifies that it fulfills the conditions of the previous theorem. Note that both E_R and E_N do not satisfy the requirements of Theorem 3.3.1.

Rains showed in a seminal paper [238] that the previous two measures can be combined as

$$E_{\text{Rains}}(\rho) = \min_{\sigma \in \mathcal{D}} \left(S(\rho||\sigma) + \log_2 \|\sigma^{T_B}\| \right),$$

providing an upper bound to the distillable entanglement. Note that here the minimum is taken over *all* states, not just the separable ones. The Rains bound gives an upper bound to the PPT distillable entanglement, that is the entanglement that can be distilled via PPT preserving protocols. Since these protocols include LOCC operations, the Rains bound provides also an upper bound to E_D. Despite this, E_{Rains} is probably the strongest known upper bound known on E_D. Note that when $\sigma = \rho$ in the definition, we simply recover E_N. A weaker bound can also be obtained by minimising just over the PPT states, so that the last term vanishes. The resulting quantity is known the relative entropy of entanglement with respect to PPT states [239, 241]

$$E_R^{PPT}(\rho) = \min_{\sigma \in \mathcal{P}} S(\rho||\sigma).$$

Measures that satisfy the requirements of Theorem 3.3.1 are the regularised version E_R^{∞} of the entropy of entanglement E_R and the regularisation of E_R^{PPT}, $E_R^{PPT\infty}$. There is some evidence that $E_{\text{Rains}} = E_R^{PPT\infty}$, based on the equality for Werner states, although all that is known is that for qubits $E_R^{PPT\infty} \leq E_{\text{Rains}}$ [7, 8, 164].

Lower bounds to the entanglement of distillation are much harder to obtain. One way of obtaining a lower bound is by providing an explicit distillation protocol (see Section 3.4) and calculating the rate. The most important lower bound up to date is

given by the hashing inequality [21, 70, 137]

$$E_D(\rho) \geq E_{D_\rightarrow}(\rho) \geq \max\{0, S(\rho_B) - S(\rho), S(\rho_A) - S(\rho)\}. \tag{3.7}$$

Here $E_{D_\rightarrow}$ is the one-way distillable entanglement, that is the entanglement of distillation where classical communication is only allowed in one direction (for instance only from Alice to Bob). Note that this relation also has important implications on the theory of quantum channel capacities. For some states the value of E_R coincides with this bound, and thus allows for exact calculation of E_D. Examples will be given in the next section.

From our treatment, it is easy to see that (see also [54, 230] for excellent treatments on entanglement ordering)

$$E_F \geq E_R, E_C \geq E_R^\infty, E_R^{PPT} \geq E_R^{PPT\infty} \geq E_D$$

and

$$E_N, E_R^{PPT} \geq E_{\text{Rains}} \geq E_D.$$

As an example, in Figure 3.1 we have plotted known values of entanglement measures for the Werner states $(d = 3)$. The Werner states [138, 321] are states of the form

$$\rho = \frac{1}{d^2 + \beta d}(\mathbb{1} + \beta F),$$

with $-1 \leq \beta \leq 1$, which are entangled $\beta < -1/d$ or $-1 \leq \text{Tr}(\rho F) < 0$. We will study this class of states extensively in the context of distillability in Section 4.3, see also Section 4.1. Because of their prominent symmetry the value of some important entanglement measures can be calculated exactly. In particular we have $E_R = E_R^{PPT}$ and $E_{\text{Rains}} = E_R^{PPT\infty}$ [7, 8, 310]. Despite this, an analytical expression for both E_C and E_D is still out of reach. It is not even known whether the distillable entanglement for all entangled Werner states is strictly positive (see Section 4.3)! In Section 3.4 we redraw the graph for $d = 2$ for which the situation is somewhat simplified and for which good lower bounds are known on E_D.
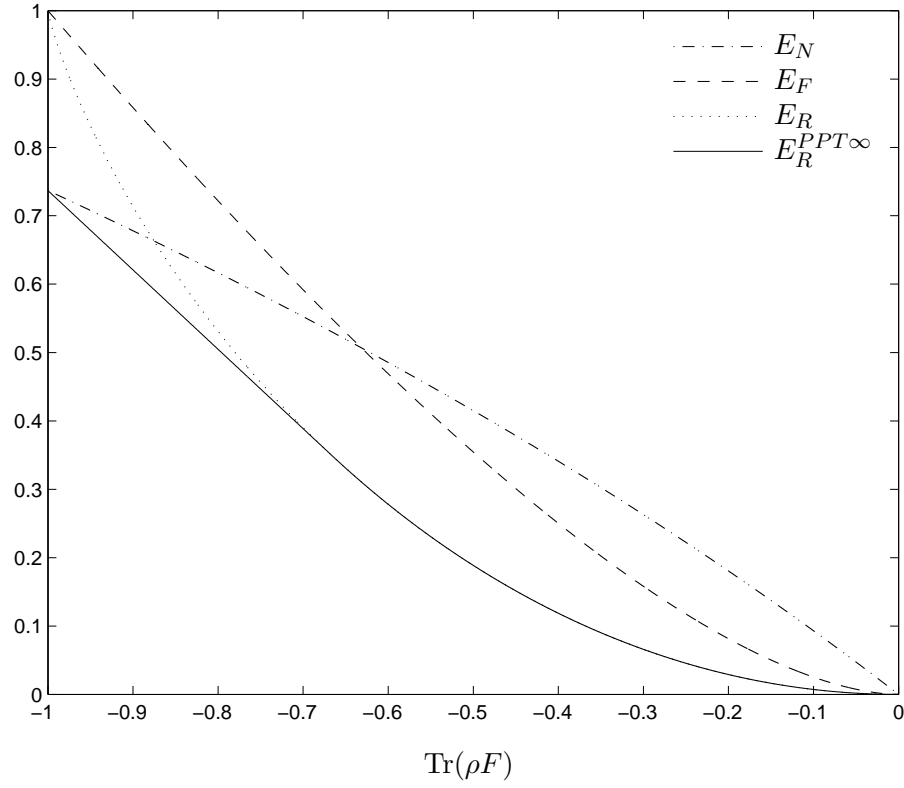
Figure 3.1: Entanglement measures E_N, E_F, $E_R = E_R^{PPT}$ and $E_{\mathrm{Rains}} = E_R^{PPT\infty}$ as a function of the parameter $\mathrm{Tr}(\rho F)$ for the Werner states.

3.3.3   Irreversibility

Bound entanglement

For pure states, entanglement is reversible in the sense that $E_D(\psi) = E_C(\psi) = E(\psi)$ for all pure states ψ. In this section we will show that this is not necessarily the case for mixed states. The first indication of this was the discovery of bound entangled states, that is entangled states from which no entanglement can be distilled at all [134]. The class of bound entangled states includes the set of PPT states. We present the direct proof from Ref. [138].

Theorem 3.3.3. *For any PPT state ρ the distillable entanglement is zero. PPT states are therefore bound entangled.*

Proof. As we have seen in Section 3.1 the set of PPT preserving protocols includes all LOCC transformations. Therefore LOCC cannot map a PPT state to an NPT state. Now we prove that PPT states are bounded away from the maximally entangled state. Let ρ be a d-level PPT state. We have

$$\mathrm{Tr}\,\rho P_+ = \mathrm{Tr}\,\rho^{T_B} P_+^{T_B} = \frac{1}{d}\,\mathrm{Tr}\,\rho^{T_B} F, \tag{3.8}$$

now since ρ is PPT, $\tilde{\rho} = \rho^{T_B}$ is also a legitimate state and thus

$$\mathrm{Tr}\,\rho P_+ = \frac{1}{d}\,\mathrm{Tr}\,\tilde{\rho} F \leq \frac{1}{d}, \tag{3.9}$$

where the inequality follows because the swap operator F has eigenvalues ± 1 only, and therefore has a mean smaller than one on any state. Thus whatever LOCC protocol we apply, PPT states can never achieve a higher overlap than $\frac{1}{d}$ with the maximally entangled state. Note that $\frac{1}{d}$ can be achieved by a product state. $\square$

We come back to the question of the existence of NPT bound entanglement in Chapter 4. Now the above theorem would imply irreversibility if we could prove that $E_C(\rho) \geq 0$ for PPT entangled states ρ. However likely this might seem, it is not straightforward to prove this formally. This is because, all we know for entangled states is that $E_F(\rho) > 0$, but in the asymptotic regime, it might be possible to construct PPT entangled states with an arbitrary small amount of entanglement. In Ref. [302] Vidal

and Cirac obtained the following lower bound on E_C (the proof is straightforward and we omit it here).

Theorem 3.3.4. *Let P denote the projector onto the range of a state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$. If*

$$\langle ef | P^{\otimes N} | ef \rangle \leq \alpha^N,$$

for all product vectors $|ef\rangle \in \mathcal{H}_A^{\otimes N} \otimes \mathcal{H}_B^{\otimes N}$, then $E_C \geq -\log_2 \alpha$.

This lower bound is relatively easy to calculate for some states [302, 303], in particular it was shown to be positive for some bound entangled state. The breakthrough however came with Ref. [331] which showed that $E_C(\rho) > 0$ for all entangled states. Note that this was the one crucial piece missing in the original definition of entanglement (see Section 1.2). The proof is relatively elaborate and proceeds in two steps. First a functional G is derived which is positive on all entangled states and zero on all separable states. Although this quantity G is by no means easy to evaluate, it serves the purpose as it is a lower bound to E_C.

Generic irreversibility: maximally correlated states

Irreversibility in entanglement transformation is not limited to bound entangled states. Consider for instance the class of maximally correlated states (MCS) [239, 241] which can be written as

$$\rho = \sum a_{ij} |ii\rangle\langle jj|.$$

A necessary and sufficient condition for a state ρ to be equivalent to a MCS after a possible local unitary transformation is given in Ref. [125]. The tag MCS reflects that when both parties perform the same measurement, they will obtain the same result. The Rains bound for this state is relatively easy to calculate and one obtains [47, 239, 241, 329]

$$E_{\text{Rains}}(\rho) = S(\rho_A) - S(\rho) = E_R(\rho) = E_R^{PPT}(\rho) = E_R^{PPT\infty}(\rho),$$

and by virtue of an explicit distillation protocol it can be proven [238, 240] that this value equals the PPT distillable entanglement. Note that the relative entropy is additive when acting on maximally correlated states. In view of the hashing inequality we have:

Theorem 3.3.5. *The distillable entanglement of a maximally correlated state ρ is given by*

$$D(\rho) = S(\rho_A) - S(\rho) = E_R(\rho).$$

Next we derive a sufficient condition for the additivity of the entanglement of formation, which allows for an exact expression of the entanglement cost E_C of some MCS. Central is the notion of an entanglement breaking map [142, 256, 267], this is a map $\mathcal{M} : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_{B'})$ such that for all $\rho \in \mathcal{L}(\mathcal{H}_A) \otimes \mathcal{L}(\mathcal{H}_B)$ the state $\mathbb{1}_B \otimes \mathcal{M}(\rho)$ is separable. A map $\mathcal{M}$ is entanglement breaking if and only it can be written as

$$\mathcal{M}(\sigma) = \sum_i \mathrm{Tr}(X_i \rho)\sigma_i,$$

where $X_i \geq 0$ and $\sum_i X_i = \mathbb{1}$ and $\{\sigma_i\}$ is some set of density operators. With this we have [307] the following theorem.

Theorem 3.3.6. *Let V be a subspace of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$. Define a map $\mathcal{M} : \mathcal{L}(V) \to \mathcal{L}(\mathcal{H}_{A_1})$ by*

$$\mathcal{M}(\rho_V) = \mathrm{Tr}_{B_1} \rho_V$$

for all $\rho_V \in \mathcal{L}(V)$. If $\mathcal{M}$ is entanglement breaking, then

$$E_f(\rho_V \otimes \sigma) = E_f(\rho_V) + E_f(\sigma)$$

for all $\rho_V \in \mathcal{L}(V) \subset \mathcal{L}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1})$ and all $\sigma \in \mathcal{L}(\mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2})$. In particular, for all $\rho_V \in \mathcal{L}(V)$ we have $E_C(\rho_V) = E_F(\rho_V)$.

Let us now apply this to the maximally correlated states [140, 307, 312]. Any MCS is supported on the span of $\{|ii\rangle\}$, so let $|\psi\rangle = \sum_i |\psi_i\rangle_C |ii\rangle_{A_1 B_1}$, then

$$\mathbb{1}_C \otimes \mathcal{M}(|\psi\rangle\langle\psi|) = \mathrm{Tr}_{B_1}(|\psi\rangle\langle\psi|) = \sum_i |\psi_i\rangle\langle\psi_i|_C \otimes |i\rangle\langle i|_{A_1}.$$

In other words, the map $\mathcal{M}$ associated to V is entanglement breaking, and thus $E_F(\rho) = E_C(\rho)$ for all MCS ρ. The entanglement of formation can be calculated exactly for qubits, and comparing the entanglement cost with the entanglement of distillation, one obtains generic irreversibility for all two-qubit MCS. In view of these results it would be worthwhile investigating whether a closed expression for the entanglement of formation can be obtained for MCS of arbitrary dimension. There is no reason however to suspect that irreversibility in higher dimension would not be generic.

Reversibility and Distinguishability

The previous section raises the question if there are any reversible mixed states. Trivial examples constitute the so-called quasi-pure states [91, 123, 270, 312] of the form

$$\rho = \sum_i p_i |ii\rangle\langle ii| \otimes |\psi_i\rangle\langle\psi_i|.$$

A simple measurement of both parties in the $\{|i\rangle\}$ basis will result in the collapse $\rho \rightarrow |ii\rangle\langle ii| \otimes |\psi_i\rangle\langle\psi_i|$, therefore $E_C(\rho) = E_D(\rho) = \sum_i p_i E(\psi_i)$. Note that the process of identifying the tag $|ii\rangle\langle ii|$ is reversible in the asymptotic regime, hence the reversibility. More general quasi-pure states take the form

$$\rho = \sum_i p_i \rho_i \otimes |\psi_i\rangle\langle\psi_i|,$$

with $\{\rho_i\}$ a set of separable and orthogonal states which are locally distinguishable. This latter condition is necessary as there are separable orthogonal states that cannot be distinguished locally [22, 141, 330] with probability one. It seems to be an open question whether there are reversible truly mixed states which are not quasi-pure (see also [150]).

Distinguishability has far deeper implications on distillation. We start with an example [48, 101]. Let $\{|B_{ij}\rangle\}$ denote the set of the four Bell states $\frac{1}{2}(|00\rangle \pm |11\rangle)$ and $\frac{1}{2}(|01\rangle \pm |10\rangle)$, and define

$$\rho_n = \frac{1}{4} \sum_{i,j=0}^{1} |B_{ij}\rangle\langle B_{ij}|^{\otimes n}.$$

We focus on the case where n is even. The state ρ_2 is separable and therefore $\rho_2^{\otimes m}$ is also separable. The relative entropy for $n = 2m$ is bounded by

$$E_r(\rho_{2m}) \leq S(\rho_{2m}||\rho_2^{\otimes m}) = 2m - 2.$$

This last step follows by direct verification. Now the set of two copies of all four Bell states can be locally distinguished [313], so that by sacrificing two copies, one can distill $2m-2$ ebits from ρ_{2m}. Since the entanglement of distillation is bounded by the relative entropy we have $E_r(\rho_{2m}) = E_D(\rho_{2m}) = 2m-2$. Other examples of using explicit LOCC distinguishing in a distillation process can be found in Ref. [102].

The link between distinguishability and distillation can be formalised as follows. First we start by recalling the Holevo bound (see for instance [214], Chapter 11 and

12). Suppose Alice prepares a state ρ^x with probability p_x and hands it over to Bob. He performs a measurement, with measurement outcome y. The random variable X with values x is characterised by the entropy $S(X) = -\sum_x p_x \log_2 p_x$ and similarly Y is characterised by $S(Y) = -\sum_y p_y \log_2 p_y$. The joint entropy is then characterised by $S(X, Y) = -\sum_{x,y} p(x, y) \log_2 p(x, y)$. With these definitions the mutual information is defined by $S(X : Y) = S(X) + S(Y) - S(X, Y)$ and quantifies how much information X and Y have in common. The accessible information I_{acc} is the maximum mutual information over all possible measurement strategies of Bob. As an example, suppose that Alice prepares a state in d possible orthogonal states, then clearly Bob can always access this information completely, and therefore $I_{\text{acc}} = \log_2 d$. When Alice prepares non-orthogonal states, this value will be smaller. Now, the Holevo bound is an upper bound to the accessible information:

$$S(X : Y) \leq I_{\text{acc}} \leq S(\rho) - \sum_x p_x S(\rho^x) \leq N$$

with $\rho = \sum_x p_x \rho^x$, and $N = \log_2 \dim \mathcal{H}$. In particular it follows that N qubits can be used for information transmission of at most N bits. Now we generalise this in the scenario that Charlie prepares a bipartite state and gives a half both to Alice and Bob, who can only perform LOCC [12, 103, 143]. Note that the local accessible information is bounded by the accessible information $I_{\text{acc}}^{\text{LOCC}} \leq I_{\text{acc}}$. A Holevo-like bound can be obtained in this way (we present a strongly simplified version):

Theorem 3.3.7. *The local accessible information of a quantum state $\rho \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is bounded by*

$$I_{acc}^{LOCC}(\rho) \leq N - E_F(\rho) - E_F(\tilde{\rho}),$$

with $N = \log_2 \dim \mathcal{H}$. Here $\tilde{\rho}$ is the residual state, the state left-over by Alice and Bob after a particular measurement process. The amount of entanglement $E_F(\tilde{\rho})$ that may be extracted during the process satisfies $E_{distilled} \leq E_F(\tilde{\rho})$.

Thus to some extent, the entanglement (both initial and final) and local accessibility are complementary quantities. In our example above, the local accessible information $I_{\text{acc}}^{\text{LOCC}}(\rho_{2m}) = 2$, while $N = 4m$ and $E_F(\rho_{2m}) = 2m$, so that $E_{\text{distilled}} \leq E_F(\tilde{\rho}) \leq 2m - 2$ in the process of information extraction. The bound is here saturated; as in the process

of information extraction, we distill $2m - 2$ ebits and the extraction of locally accessible information is in this case the best distillation procedure (see above). The upper bound of local accessible information hence gives an upper bound on the entanglement of distillation that can be obtained through local distinguishing (see also [262]). We will encounter distillation protocols based on local distinguishing in the next section.

3.4 Some important distillation protocols

In this section we review some important distillation protocols. We analyse them in some detail for bipartite qubit systems, and only point to the relevant literature for higher level systems as already in the bipartite qubit scenario the main principles of distillation can be captured. From a practical point of view, it is also probably the most interesting. Note however that we discuss distillation protocols from a theoretical point of view, with disregard for practical limitations and operational simplicity. The foundations of all current distillation protocols have been set out in two brilliant papers Ref. [20, 21] which we will follow closely. It is somehow remarkable how relatively little progress has been made since these were originally published.

3.4.1 Recursive protocols

The recurrence protocol (IBM protocol)

Being the first protocol [20, 21], the recurrence protocol is also the simplest. Alice and Bob start with a large pool of identical qubit states with fidelity $Y = \text{Tr}(\rho P_+) \geq 1/2$. In every round of the protocol two pairs $\rho^{\otimes 2}(Y)$ get consumed, and with some probability, a single pair $\rho'(Y')$ is produced with $Y' > Y$. Doing this a large number of times, the original pool of states $\rho(Y)$ will be transformed into a smaller pool of states $\rho'(Y')$. Repeating the protocol, this time on the new pool of states, they can increase the fidelity further, and so on (hence the name recurrence protocol).

So let Alice and Bob take two identical pairs with fidelity Y. In the first step of the protocol, they will bring both pairs in the standard isotropic form (see also Chapter 2 and Section 4.1)

$$\rho' = \frac{1}{4 + \beta}(\mathbb{1} + \beta P_+).$$

States of this form are invariant under local bilateral unitaries $\rho' = (U \otimes U^*)\rho'(U \otimes U^*)^\dagger$ and it follows that we can bring any state into the isotropic form by performing a random local unitary (this is the so-called twirling operation) without changing its fidelity.

The unitary XOR (or CNOT) [214] defined by

$$U_{\text{XOR}} = |00\rangle\langle00| + |01\rangle\langle01| + |11\rangle\langle10| + |10\rangle\langle11|,$$

behaves just like a classical XOR, flipping the second bit, conditionally on the first. Now the second step of the recurrence protocol consists of both parties implementing the local unitary XOR on their two halves. For the sequel we will call the first pair the source pair and the second pair the target pair. This local unitary operation called BXOR (bilateral XOR) entangles both Alice's and Bob's local halves, while it leaves the global entanglement between Alice and Bob unaltered.

Finally, Alice and Bob measure the second pair in the basis $\{|0\rangle, |1\rangle\}$. If the outcomes of their measurement coincide, it is not so hard to show that the fidelity of the first pair will change as

$$Y' = \frac{9Y^2 + (1-Y)^2}{9Y^2 + 6Y(1-Y) + 5(1-Y)^2}.$$

Figure 3.2 illustrates this relation, and it can be seen that the fidelity strictly increases when $Y > 1/2$. The first pair will no longer be isotropic, so that for further rounds in the protocol, the first step (twirling) will have to be repeated. When the measurement outcomes do not coincide, the first pair has to be disregarded, and the protocol was unsuccessful. It is important to note at this point that the exchange of the measurement outcomes requires two-way communication.

As remarked at the start of this section, this round of the protocol will have to be repeated many times, until a sufficiently large pool of states with fidelity Y' has been obtained. Then a new round can be started, using the new pool of states. In this way the recurrence protocol is able to transforms states with fidelity $Y > 1/2$ into states with fidelity arbitrary close to one. The probability of doing so however tends to zero as $Y \to 1$, as in every round at least half of the states are disregarded.
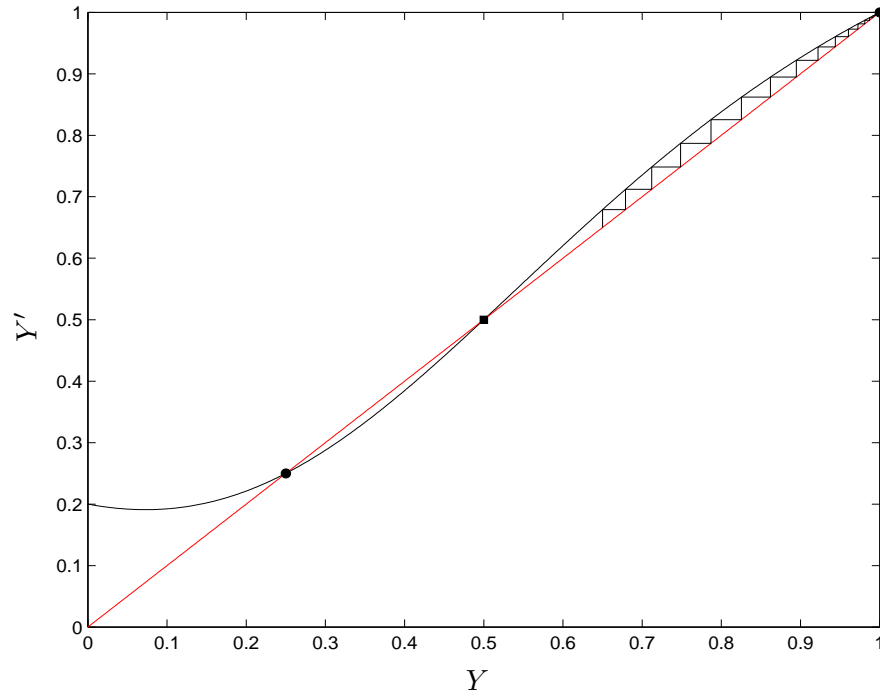
Figure 3.2: One iteration in the recurrence protocol. The curved line is $Y'(Y)$, while the staircase curve illustrates the evolution of the fidelity through repeated recurrence rounds, starting with $Y = 0.65$. The black dots denote attractive fix-points, while the black square denotes a repulsive fix-point. This figure is an adaption of a similar one published in Ref. [5].

The QPA protocol (Oxford protocol)

The QPA protocol [69, 194] was introduced in the context of quantum cryptography (Quantum Privacy Amplification) and is an improved version of the recurrence protocol. It achieves a certain fidelity with higher probability and does not require twirling. In fact it works in an identical fashion as the recurrence protocol, except that the twirling operation is replaced by a rotation. For completeness, the protocol consists of the following steps:

1. Denote $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ and define a unitary operator $R = |\phi\rangle\langle 0| - i|\phi^*\rangle\langle 1|$. Then Alice implements R on each of her qubits and Bob implements $R^\dagger$ on his qubits. It can be verified that this amounts to ordering the coefficients p_{ij} (see below), such that $p_{00} \geq p_{01} \geq p_{10} \geq p_{11}$ [68] .

2. The parties implement the unitary BXOR on their two halves.

3. Alice and Bob measure the second pair in the basis $\{|0\rangle, |1\rangle\}$ and keep the first pair if and only if their measurement outcomes coincide.

   To see that this is a distillation protocol, let us write an arbitrary state in the Bell basis

$$\rho = \sum_{i,j=0}^{1} p_{ij}|B_{ij}\rangle\langle B_{ij}| + \sum_{i,j\neq k,l}^{1} p_{ij,kl}|B_{ij}\rangle\langle B_{kl}|,$$

with

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \qquad |B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Here the first index will be called the phase index, and the second the shift index.

In this way, we can describe one step in the protocol as the mapping $\{p_{ij}, p_{ij,kl}\} \rightarrow \{\tilde{p}_{ij}, \tilde{p}_{ij,kl}\}$. Now by going through the algebra it can verified that the coefficients $\tilde{p}_{ij}$ only depend on p_{ij}, more precisely:

$$\tilde{p}_{00} = \frac{p_{00}^2 + p_{11}^2}{P}, \qquad \tilde{p}_{10} = \frac{2p_{01}p_{10}}{P},$$
$$\tilde{p}_{01} = \frac{p_{01}^2 + p_{10}^2}{P}, \qquad \tilde{p}_{11} = \frac{2p_{00}p_{11}}{P},$$

with $P = (p_{00} + p_{11})^2 + (p_{01} + p_{10})^2$. It is not completely straightforward, but it can be proven [194] that when $p_{00} = \text{Tr}(\rho P_+) > 1/2$ the protocol converges to P_+ (that is $p_{00} \to 1$).

Local permutations

Several improvements of the early recursive protocols have been proposed [157, 201, 209, 210, 216]. It has also been realised that the recurrence and the QPA protocol can be interpreted as coming from a quantum stabilizer code, and how to convert an arbitrary quantum stabilizer code to a distillation protocol [3, 208, 315]. As it turns out, all these different schemes can to a large extend be captured in the so-called local permutations schemes [68, 155].

The main idea is to start with n pairs every round, and at the end measure m pairs. Such a protocol will be called an $[n, m]$-protocol, the QPA and recurrence protocols are thus $[2, 1]$ protocols. Naturally, for $n > 2$ the XOR operation will have to be replaced by some multipartite unitary entangling operator. One way of doing this stems from analysing the BXOR operation in a bit more detail. Note that the XOR operation can be written as

$$U_{\text{XOR}}|i\rangle|j\rangle = |i\rangle|i \oplus j\rangle,$$

with $\oplus$ addition modulus 2. From this follows that the BXOR operation acts on two Bell states as (note that as usual the two Bell states are shared by both parties) [311]

$$U_{\text{BXOR}}|B_{ij}\rangle|B_{kl}\rangle = |B_{i\oplus k,j}\rangle|B_{k,j\oplus l}\rangle.$$

Thus although BXOR is an entangling operation, it happens to be non-entangling on Bell states[4]. In view of the above we write $ijkl \xrightarrow{\text{BXOR}} i'k'j'l'$ and interpreting $ijkl$ as a bitstring, we can attach a number from 1 to 4^2 to it. It is then not so hard to show that in this sense the BXOR corresponds to a permutation of 4^2 elements. Generalising to n pairs, one can consider permutations of 4^n elements, such that the corresponding unitary is local. The aim of working with this restricted set of unitaries, rather than say, all local unitaries or even all permutations is to make optimisation easier. Furthermore,

---

[4]To see that BXOR, or thus XOR is entangling it is sufficient to consider an example such as $U_{\text{XOR}}(|00\rangle + |10\rangle) = |00\rangle + |11\rangle$.

an elegant closed expression for these special permutations is known [68]. The problem of finding an optimal $[n, m]$-protocol is highly non-trivial, as a trade off has to be found between the increase in fidelity and the probability at which this happens. Also, in general, the choice of the permutation will be state dependent. Once a suitable permutation has been found, the distillation protocol is identical to the QPA protocol, except that in the second step the BXOR need to be replaced with the corresponding local unitary and in the third step, m pairs need to be measured.

Note that recurrence protocols can be readily generalised to higher level states ρ with $\text{Tr}(\rho P_+) > 1/d$ by replacing the XOR by some multilevel entangling unitary [2, 28, 131, 202].

3.4.2   Hashing and breeding

The hashing protocol [21, 269], unlike the recurrence schemes has a strictly positive yield for Bell diagonal states with $S(\rho) \leq 1$. Somewhat contradictorily, the protocol does only need 1-way communication. In this section we present a simplified version, the breeding protocol [20], which assumes that Alice and Bob share initially $S(\rho)$ pure singlets (we call them here pre-distilled singlets) per pair of ρ. However as it turns out, both protocols give rise to the same yield.

In the breeding protocol Alice and Bob share an arbitrarily large amount n of identical Bell diagonal states:

$$\rho^{\otimes n} = \sum_{k_1, l_1 \cdots k_n, l_n} p_{k_1, l_1 \cdots k_n, l_n} P_{k_1 l_1} \otimes \cdots \otimes P_{k_n l_n},$$

with $P_{ab} = |B_{ab}\rangle\langle B_{ab}|$. Note that any state can be made Bell diagonal by a certain discrete twirl operation (see Section 4.1). The main idea of the breeding/hashing protocols is now to interpret the above as Alice and Bob sharing $P_{k_1 l_1} \otimes \cdots \otimes P_{k_n l_n}$ with probability $p_{k_1, l_1 \cdots k_n, l_n}$. This way of reasoning is perfectly valid as the density operator contains all physical observable information, independently of the preparation procedure, and the state $\rho^{\otimes n}$ can be thought of as prepared in this way. The goal of Alice and Bob is then to identify the specific sequence $(\vec{k}, \vec{l}) = (k_1, \cdots, k_n, l_1, \cdots l_n)$, after which Bob can simply apply local unitary transformations to obtain $P_{00}^{\otimes n}$.

The breeding protocol uses pre-distilled singlets as target states for BXOR opera-

tions to gain information on the source states characterised by the sequence $(\vec{k}, \vec{l})$. If Alice and Bob implement a BXOR with a pure target $|B_{0m}\rangle$:

$$U_{\text{BXOR}}|B_{kl}\rangle|B_{0m}\rangle = |B_{k,l}\rangle|B_{0,l\oplus m}\rangle,$$

then the shift index of the target pair toggles when the source pair has shift index $l = 1$, while the source pair remains unchanged. So when Alice and Bob perform BXOR operations on each pair of a subset of n' pairs with a pure singlet as a fixed target state, they can identify the number of source pairs with shift index 1, by measuring (locally) the shift index of the target state. Thus, this procedure allows them to identify the parity of the shift indices in the subset. Similarly, by replacing BXOR by a different local unitary, they can determine the parity of the phase indices in the subset.

The question is now how many parity checks are needed to gain complete information of the sequence $(\vec{k}, \vec{l})$. This is important, as each parity check consumes 1 pair of their initially pre-distilled singlets. A total random sequence of n pairs needs $2n$ parity checks to uniquely identify, so in doing so we would lose more entanglement than we gain. However, for $n \to \infty$ the sequence will belong to the class of $2^{nS(\rho)}$ typical sequences with probability going to one. It can be shown that the probability that two different sequences have the same parities after r checks on random subsets is smaller than $\frac{1}{2^r}$. So typically, after every parity check the list of typically sequences reduces by a factor $\frac{1}{2}$ and thus $r = nS(\rho)$ parity checks will be sufficient to identity the sequence in the asymptotic regime (see Ref. [20] for a rigorous analysis). The yield of the breeding protocol is therefore

$$\lim_{n\to\infty} \frac{n - nS(\rho)}{n} = 1 - S(\rho),$$

which agrees with the hashing inequality (3.7). Both hashing and breeding can be generalised to multilevel systems [311]. As a side remark, note that there is a close correspondence between 1-way distillation protocols and quantum error correcting codes. The most important implication of this correspondence is the quantum noisy coding theorem, which follows from the hashing inequality (recall that this inequality gives a lower bound on the 1-way distillable entanglement) [21, 70, 137, 269].

In Figure 3.3, the value of distillable entanglement by the hashing protocol (denoted H) has been plotted for the Werner states. As can be seen from the figure, the hashing
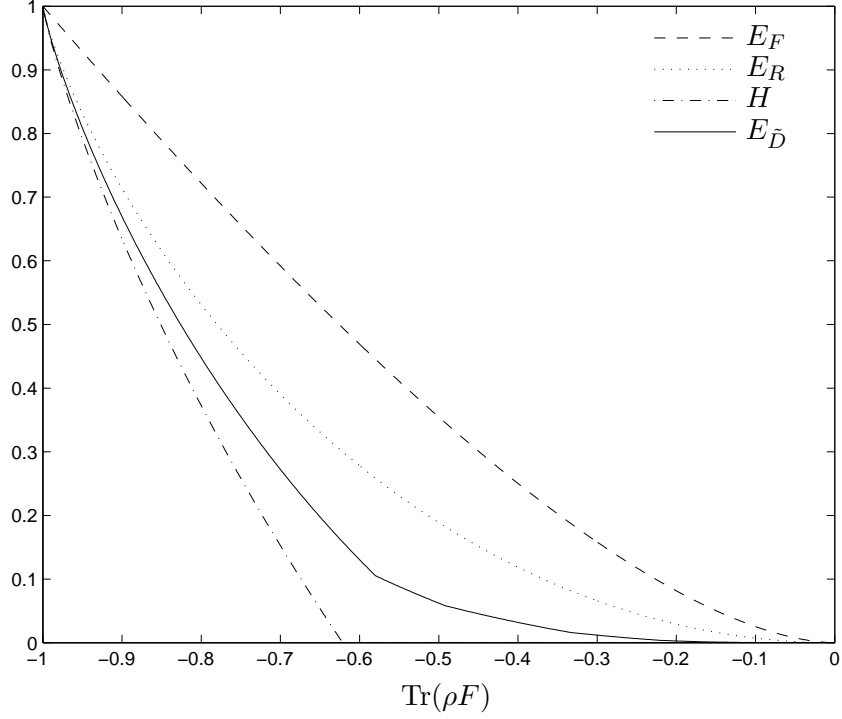
Figure 3.3: Entanglement measures E_F and $E_R = E_R^{PPT} = E_{\text{Rains}} = E_R^{PPT\infty}$ as a function of the parameter $\text{Tr}(\rho F)$ for the Werner states. H and $E_{\tilde{D}}$ are the distillation rates of the hashing protocol and the protocol of Ref. [156] respectively (the data was obtained courtesy of E. Hostens).

protocol works only for $\mathrm{Tr}(\rho F) < -0.62$. This can be bypassed by preceding the hashing protocol by a few recurrence steps, increasing the fidelity above this threshold. While the recurrence protocol exploits two-way communication, only the hashing protocol is a proper asymptotic protocol. By introducing two-way communication on the asymptotic level, small improvements can be made [156, 308]. The currently best known distillation rate for the Werner states $E_{\tilde{D}}$ has been plotted in Figure 3.3.

CHAPTER 4

Distillability, activation and NPT bound entanglement

Having encountered PPT bound entangled states in the previous chapter, this chapter deals with the more general question of distillability of general quantum states. We call a state distillable if and only if the distillable entanglement is strictly larger than zero. In three seminal papers [131, 133, 134] the Horodeccy derived the fundamentals of the theory of distillability. Namely they showed that (i) any two-qubit entangled state can be distilled; (ii) any general d-level state ρ is distillable if and only if there exists a two-qubit subspace on which $\rho^{\otimes n}$ is entangled for some n; (iii) any state violating the reduction criterion can be distilled. The second statement has a number of nontransparent reformulations. Here we present a unified presentation of these and other distillability theorems, using tools borrowed from the separability problem. This allows us to systematically construct positive maps, with the same properties as in (iii) of the reduction criterion [59]. We give several other applications, including a numerical method for checking distillability which we apply to estimate the volume of distillable states. (Sections 4.1-4.2).

In the next section we address the question of NPT bound entanglement in detail. After reviewing previous results [72, 83, 316], we show that this question is equivalent

to a specific Schmidt number problem and to a separability problem. In particular, we show it is equivalent to the existence of a certain class of PPT entangled states. We end this section with a set of one parameter states which we conjecture to exhibit all forms of distillability (the rainbow states) [60].

As bound entangled states are not directly useful for typical quantum information tasks such as teleportation, the question arises whether they have any non-classical use at all. We will see that bound entanglement can be activated. That is, bound entanglement can be released with the help of other (possible bound) entangled states. A first activation-like effect was presented in Ref. [149], but the main results were obtained in Ref. [87, 203]. This is the topic of Section 4.4.

4.1   Classic results

4.1.1   States symmetric under local unitaries

In previous chapters we have encountered the isotropic states and the Werner states. These states are invariant under certain local unitaries, and because of their symmetry they have been exhaustively used in the study of distillability. In this section, we review briefly the general theory of states symmetric under local unitaries, as developed in Ref. [309].

Let G_0 be a subgroup of the unitaries, or possibly the whole group of the unitaries. Then we can define the group G of the unitaries consisting of all pairs of the form $U \otimes U'$ acting on a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, where $U \in G_0$ and U' is some given function of U. The set of bipartite states left invariant by the group G will also be denoted as UU'-invariant instead of G-invariant. An arbitrary state can be projected onto an UU'-invariant state by twirling it

$$\mathcal{T}_G(\rho) = \int_G dU (U \otimes U') \rho (U \otimes U')^\dagger.$$

Here the integral is performed according to the Haar measure on G_0. In particular, for a finite group, the integral can be replaced by the sum

$$\mathcal{T}_G(\rho) = \frac{1}{|G|} \sum_{U \in G} U \otimes U' \rho (U \otimes U')^\dagger.$$

The commutant G' of the group G is defined as the set of all operators invariant under G-twirling, or equivalently the set of all operators A such that $[U, A] = 0$ for all $U \in G$. It follows that the set of bipartite states left invariant by G is just the intersection of the state space with the commutant G' of the group G. Note that there always exist a finite basis of operators $B(G')$ spanning the commutant G'. Now for any operator C it is straightforward to check that

$$\text{Tr}(\mathcal{T}_G(\rho)C) = \text{Tr}(\rho\mathcal{T}_G(C)).$$

This relation has a number of important consequences:

1. A G-invariant state ρ is uniquely determined by the expectation values $\text{Tr}(\rho A)$ for all $A \in G'$. In particular, if $B(G')$ is finite, then the set of G-invariant states can be characterised by a finite set of parameters $g_A = \text{Tr}(\rho A)$, for all $A \in B(G')$.

2. For an arbitrary state ρ, the parameters $g_A = \text{Tr}(\rho A)$, for all $A \in B(G')$, are invariant under twirling. From the previous point it follows that in order to calculate the image of ρ under twirling it is sufficient to calculate these parameters.

3. Suppose we need to calculate an extreme for some G-invariant state ρ such as $\min_C \text{Tr}(\rho C)$, where the operators C belong to some set $\mathcal{C}$. It is then sufficient to minimise over the (smaller) set) $\mathcal{T}_G(\mathcal{C})$.

For the Werner states [321], which are UU-invariant, the commutant is spanned by $\mathbb{1}$ and F. The isotropic states [131, 241] are UU^*-invariant and a basis is given by $\mathbb{1}$ and P_+. Note that for qubits, the Werner and isotropic states are related via a local unitary, while this does not hold for higher dimensions. As we have seen in the previous section, some distillation protocols make extensive use of twirling. As remarked in Section 2.4.1 for the Werner and isotropic states, it can be shown that the twirl can be written as a finite sum ([21, 83]). In practice however, twirling can be done simply by performing a single random UU or UU^* transformation and forgetting which specific unitary was used.

The Bell diagonal states encountered in the previous chapter are invariant under the group

$$G = \{\mathbb{1} \otimes \mathbb{1}, -\sigma_x \otimes \sigma_x, -\sigma_y \otimes \sigma_y, -\sigma_z \otimes \sigma_z\},$$

with as usual $\sigma_x, \sigma_y, \sigma_z$ the Pauli matrices. A generalisation of Bell diagonal states and their symmetry group for arbitrary dimensions is presented in Ref. [311].

From basic symmetry groups one can generate others using tensor products. Consider the case where we have two symmetry groups $G = \{U \otimes U'\}$ and $K = \{V \otimes V'\}$ acting respectively on $\mathcal{H}_1 = \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_2 = \mathcal{H}'_A \otimes \mathcal{H}'_B$. Let B_G and B_K be a basis for the UU'- and the VV'-invariant states respectively. Then a basis for the $UU'VV'$-invariant states acting on $\mathcal{H}_1 \otimes \mathcal{H}_2$ will be given by $B_G \otimes B_K$. In what follows, we will number the systems belonging to party A with odd numbers and party B with even numbers. As an example, a basis for the $UUVV$-invariant states is given by the operators $\{\mathbb{1}_{12} \otimes \mathbb{1}_{34}, F_{12} \otimes \mathbb{1}_{34}, \mathbb{1}_{12} \otimes F_{34}, F_{12} \otimes F_{34}\}$. Imposing the extra condition that the coefficients of $F_{12} \otimes \mathbb{1}_{34}$ and $\mathbb{1}_{12} \otimes F_{34}$ should be the same, we end up with the so-called $UUVVF$-invariant states as introduced in Ref. [309], where they were used as a counterexample to the additivity conjecture for the relative entropy of entanglement. We return to this set of states in Section 4.3.

4.1.2 Fundamental theorems

In this section we present the three basic theorems (Theorems 4.1.1, 4.1.2 and 4.1.3) on distillability by the Horodeccy [131, 133, 134], as mentioned in the introduction. We also present a first result [131] on NPT bound entanglement. Because of their importance we present full proofs.

Theorem 4.1.1. *All entangled two-qubit states ρ are distillable ($E_D(\rho) > 0$).*

Proof. The proof consists of locally transforming ρ into a state ρ'', which has a singlet fraction larger than a half. In Section 3.4.2 we have seen that for such states the distillable rate is strictly positive.

Since ρ is an entangled two-qubit state it has an negative partial transposition $\rho^{T_B} \ngeq 0$. We use the same technique as in (1.7) to transform the state such that it is detectable by a suitable entanglement witness. Let us denote the eigenvector corresponding to the negative eigenvalue of ρ^{T_B} with $|\psi\rangle$, so that $\langle\psi|\rho^{T_B}|\psi\rangle < 0$. Now any vector $|\psi\rangle$ can be written as $|\psi\rangle = A \otimes \mathbb{1}|\psi_+\rangle$ (see (1.3)). With this we get

$$\text{Tr}[(A^\dagger \otimes \mathbb{1})\rho(A \otimes \mathbb{1})P_+^{T_B}] < 0.$$

Now let Alice perform a filtering operation corresponding to the Kraus operators A.
Then the state becomes

$$\rho' = \frac{(A^\dagger \otimes \mathbb{1})\rho(A \otimes \mathbb{1})}{\mathrm{Tr}[(A^\dagger \otimes \mathbb{1})\rho(A \otimes \mathbb{1})]}.$$

In this way we have transformed the state such that $\mathrm{Tr}\,\rho' F < 0$, as $P_+^{T_B} = F$. Now in
$\mathcal{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ the swap operator can be written as $F = \mathbb{1} - 2P_-$, with P_- the projector
upon the state $|\psi_-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. So that we have

$$\mathrm{Tr}\,\rho' P_- > \frac{1}{2},$$

a simple local rotation can then map ρ' onto a state ρ'' such that $\mathrm{Tr}\,\rho'' P_+ > \frac{1}{2}$. □

The next theorem is the fundamental theorem of distillation, we present a slightly
different proof as compared to Ref. [134].

Theorem 4.1.2. *A state ρ on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is distillable if and only if there exist two
dimensional projectors $P : \mathcal{H}_A^{\otimes n} \to \mathbb{C}^2$ and $Q : \mathcal{H}_B^{\otimes n} \to \mathbb{C}^2$ such that for some $n \geq 1$ the
state*

$$\rho'' = (P \otimes Q)\rho^{\otimes n}(P \otimes Q)^\dagger \tag{4.1}$$

*is entangled. Since the resulting state acts on $\mathbb{C}^2 \otimes \mathbb{C}^2$, this is equivalent to ρ'' having
a negative partial transposition.*

Proof. The condition is clearly sufficient, as when such projectors can be found, many
copies of ρ'' can be produced, and from the previous theorem it follows that these can
be distilled. Suppose now that the state ρ is distillable, and thus $E_D(\rho) = r > 0$. Let
us fix arbitrarily small $\epsilon' > 0$. From the definition of distillable entanglement (3.6), it
follows that for any $\epsilon > 0$ there exists a number n and a trace preserving LOCC Λ such
that

$$\|\Lambda(\rho^{\otimes n}) - P_+^{\otimes rn}\| < \epsilon,$$

with P_+ the maximally entangled two-qubit singlet. This implies that, by choosing ϵ
small enough, and disregarding all but one approximate copy of P_+, we can find an
LOCC protocol Λ' such that

$$\|\Lambda'(\rho^{\otimes n}) - P_+\| < \epsilon',$$

We write this LOCC protocol in the separable form (with N a normalisation factor)

$$\rho' = \Lambda'(\rho^{\otimes n}) = \frac{1}{N} \sum_i (A_i \otimes B_i)\rho^{\otimes n}(A_i \otimes B_i)^\dagger. \tag{4.2}$$

Since this is approximately P_+ we know that ρ' is entangled and we can assume that all $(A_i \otimes B_i)$ project onto the same two-qubit space. Thus every A_i and B_i can be written as

$$A_i = |0\rangle\langle\psi_{Ai}| + |1\rangle\langle\phi_{Ai}|, \qquad B_i = |0\rangle\langle\psi_{Bi}| + |1\rangle\langle\phi_{Bi}|.$$

Clearly, since ρ' is entangled, at least one term in this sum (4.2) must be entangled, for instance for $i = 1$. We denote the projector on the space spanned by $\{\phi_{A1}, \psi_{A1}\}$ as P and the projector on $\{\phi_{B1}, \psi_{B1}\}$ as Q. We have thus shown that the following two-qubit state

$$\rho'' = (A_1 \otimes B_1)\rho^{\otimes n}(A_1 \otimes B_1)^\dagger = (A_1 \otimes B_1)(P \otimes Q)\rho^{\otimes n}(P \otimes Q)^\dagger(A_1 \otimes B_1)^\dagger$$

is entangled. It follows that also the two-qubit state $(P \otimes Q)\rho^{\otimes n}(P \otimes Q)^\dagger$ must be entangled. $\qquad\square$

If the condition of the theorem is satisfied for a particular number n, then we call the state *pseudo-n-copy distillable* or in short *n-distillable* [72, 83]. This result has proven to be extremely useful and is often used as a definition of distillability. For completeness, we state the following corollary (see Ref. [72, 131]):

Corollary 4.1.1. *A state ρ on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is n-distillable if and only if there exist some local operators A and B mapping onto $\mathbb{C}^2$ such that*

$$\mathrm{Tr}(F(A \otimes B)\rho^{\otimes n}(A \otimes B)^\dagger) < 0$$

or

$$\frac{\mathrm{Tr}(P_+(A \otimes B)\rho^{\otimes n}(A \otimes B)^\dagger)}{\mathrm{Tr}((A \otimes B)\rho^{\otimes n}(A \otimes B)^\dagger)} > 1/2,$$

with P_+ and F acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Proof. This corollary follows directly from the previous theorem and the fact that any entangled two-qubit state violates both the partial transpose and reduction criterion. Via local filtering, see equation (1.7) and the subsequent discussion (see also the proof of Theorem 4.1.1), one can then transform these states such that they are detected by the witnesses F and $\mathbb{1} - 2P_+$. $\qquad\square$

Theorem 4.1.3. *All states violating the reduction criterion are distillable.*

Proof. In a similar fashion as in the proof of the previous corollary, a state ρ violating the reduction criterion can be locally transformed into a state ρ', which can be detected by the witness $\mathbb{1} - dP_+$, or

$$\text{Tr}(\rho' P_+) > \frac{1}{d}.$$

As remarked in Section 3.4.1, for such states a recurrence protocol is available. To get a finite yield, one can then use a multilevel generalisation of the hashing protocol, see Section 3.4.2.

Another way [138] of showing this is to UU^*-twirl the state ρ', after which it will become isotropic. The fidelity remains invariant under UU^*-twirling so that the state is still entangled. Now both parties apply on their half the operation $P = |0\rangle\langle0| + |1\rangle\langle1|$. This projects the state ρ' onto a two-qubit isotropic state ρ'' with $\text{Tr}(\rho'' P_+) > \frac{1}{2}$, and such states are distillable, as we have seen in the discussion of distillation protocols (Section 3.4). $\qquad\square$

The second proof implies that all states violating the reduction criterion are distillable if and only if all entangled isotropic states are. A dual result can be obtained for the partial transpose criterion and the Werner states:

Theorem 4.1.4. *All entangled NPT states can be distilled if and only if all entangled Werner states can be distilled.*

Proof. Since entangled Werner states have a negative partial transposition, one direction is trivial. To prove the other direction, note that as before, any NPT state ρ can be locally transformed into a state ρ' such that

$$\text{Tr}(\rho' F) < 0.$$

Now twirling this state, we obtain an entangled Werner state ρ'' (because $\text{Tr}(\rho' F) = \text{Tr}(\rho'' F) < 0$). If we are able to distill all Werner states, then also the original state is distillable. $\qquad\square$

In Section 4.3 we will present strong evidence that some of the entangled Werner states cannot be distilled, and hence for the existence of NPT bound entanglement.

We end this section on the fundamental theorems with a remark on finite copy distillation. We have seen that any distillable state is (pseudo)-n-copy distillable. The prefix *pseudo* reflects that if we project upon a two dimensional subspace, we are only half way through our distillation process. Indeed, in the next step we would like to repeat this procedure m times on batches of n copies of ρ, giving us m copies of the qubit pair ρ'. Finally we can use existing protocols to extract maximally entangled singlets from $\rho'^{\otimes m}$ for $m \to \infty$. Thus in general, even when a state is n-distillable we might need an infinite number of copies to get a finite yield of distillation.

It is then natural to ask whether there are any states which can be distilled using a finite number of copies, and in particular if there are any states which are single copy distillable. Clearly, pure states are single copy distillable and so are the quasi-pure states encountered in Section 3.3.3. For generic qubit mixed states, it has been proven [172, 189] that this is not possible. For qubits the best strategy to increase the entanglement of formation is transforming the state into a Bell diagonal state [173].

The explicit form of this transformation was found in Ref. [42, 298]. See Ref. [147] for bounds on single copy distillation of arbitrary level systems. Despite that in general single-copy distillation is not possible, the Horodeccy showed the existence of an effect which they called quasi-distillation [136] (see also [298]). In this scenario, it is possible to extract a pure maximally entangled singlet from some (specially constructed) single mixed state, but with probability going to zero, as the fidelity of the output state approaches this maximally entangled singlet.

The problem of finite copy distillation for more than one copy of the state has been solved for qubits in Ref. [168]. It was shown that $n \geq 2$ copies of a two-qubit mixed state ρ can be distilled into a pure entangled state if and only if the range of ρ cannot be spanned by product states. Surprisingly, this result is independent of n. This result is important as it shows that for entangled qubits, which are all 1-distillable, we need typically an infinite number of copies to distill pure entangled states. The reason is that although we can get a state with very high fidelity given a large number of copies (for instance by means of the recurrence protocol), in general this final state will still be mixed entangled. Only in the asymptotic limit of the number of copies, it is then possible to obtain a pure state.

4.2   Uniform treatment of distillability

This section contains an original contribution first published in Ref. [59]. The motivation behind this work was an attempt to answer the following questions:

> What is the special role the reduction criterion plays in the story of distillation? Are there any other positive maps with the same property? Can we find a decomposable map which is stronger than the reduction criterion, but so that all states detected by it are still distillable?

4.2.1   Borrowing tools from the separability problem

We have seen in Chapter 1 that separable states form a convex set, from which follows that there exists an entanglement witness for each entangled state. Using the Jamiołkowski isomorphism between operators and maps, this can be translated in terms of positive maps. The idea is to apply a similar reasoning to the set of distillable states. The crux is that 1-undistillable states also form a convex set. Indeed, from Theorem 4.1.2 and the linearity of the partial transpose, it follows that mixing 1-undistillable states can never yield a distillable state.

The question is now to determine the corresponding witnesses. Notice that from Theorem 4.1.2 it follows [83] that distillability is equivalent to the existence of a Schmidt rank two state $|\psi\rangle = c_1|a_1, b_1\rangle + c_2|a_2, b_2\rangle$, with $\{|a_1\rangle, |a_2\rangle\}$ two orthonormal vectors in $\mathcal{H}_A^{\otimes n}$ and $\{|b_1\rangle, |b_2\rangle\}$ two orthonormal vectors in $\mathcal{H}_B^{\otimes n}$, and some n such that

$$\langle\psi|(\rho^{\otimes n})^{T_B})|\psi\rangle = \langle\psi|(\rho^{T_B})^{\otimes n})|\psi\rangle < 0. \tag{4.3}$$

Thus $D = |\psi\rangle\langle\psi|^{T_B}$, with $|\psi\rangle$ Schmidt rank two, can be interpreted as a distillability witness. The following observation generalises this.

Observation 4.2.1. *A state ρ is 1-undistillable if and only if*

$$\mathrm{Tr}(D\rho) \geq 0$$

for all operators $D = \sigma^{T_B}$ with σ a Schmidt number two state.

This observation is compatible with the fact that PPT states cannot be distilled as D is decomposable by construction. Note that to study the phenomenon of distilla-

tion it is sufficient to characterise the 1-distillable states; n-distillable states ρ can be characterised by looking at one copy of $\rho^{\otimes n}$.

Now in a similar fashion as the separability problem and Schmidt number problem, we have to look at map Λ associated with the operator D as given by the Jamiołkowski isomorphism

$$D = d(\mathbb{1} \otimes \Lambda)P_+.$$

Let us start with the simple case where $D = |\psi\rangle\langle\psi|^{T_B}$. As D is a decomposable operator, the map Λ is decomposable and of the form

$$\Lambda = T \circ \Lambda^{CP}, \qquad \text{with} \qquad |\psi\rangle\langle\psi| = d(\mathbb{1} \otimes \Lambda^{CP})P_+.$$

What more can we say about this completely positive map Λ^{CP}? Recall that the general form of such a map is given by (see Theorem 1.2.3)

$$\Lambda^{CP}(A) = \sum_i V_i A V_i^\dagger, \tag{4.4}$$

where V_i are arbitrary operators. Now let $|\psi\rangle = \sum_{i=1}^{k} c_i|a_i b_i\rangle$ be an arbitrary Schmidt rank k state, we obtain after some algebra that the associated map[1] is given by $\Lambda^{CP}(A) = V A V^\dagger$, with

$$V = \sum_{i=1}^{k} c_i |b_i\rangle\langle a_i^*|.$$

In our case $k = 2$, so that V will have rank 2.

Let us now move to the case where $D = \sigma^{T_B}$, with σ an arbitrary Schmidt number two state. A similar line of reasoning shows that the associated map is given by $\Lambda = T \circ \Lambda^{CP}$, with Λ^{CP} a CP map with rank two Kraus operators V_i. We call maps Λ defined in this way *two-decomposable*[2]. Note that the adjoint map of a two-decomposable map is two-decomposable. It is now an easy exercise to derive the necessary and sufficient condition of one-undistillability in terms of two-decomposable maps. For completeness, we present the derivation.

Theorem 4.2.1. *A state ρ is 1-undistillable if and only if*

$$(\mathbb{1} \otimes \Lambda)(\rho) \geq 0$$

---

[1] This fact was independently obtained in Ref. [4].
[2] This term has different meaning in other contexts, such as in Ref. [179].

for all two-decomposable maps Λ.

Proof. Suppose ρ is 1-distillable, so that there exists a $D = |\psi\rangle\langle\psi|^{T_B}$, with $|\psi\rangle$ a Schmidt rank-2 vector such that $\text{Tr}(D\rho) < 0$. Using the associated map this can be written as

$$\text{Tr}[(\mathbb{1} \otimes \Lambda)(P_+)\rho] = \text{Tr}[(\mathbb{1} \otimes \Lambda^\dagger)(\rho)P_+] < 0,$$

and since P_+ is positive it follows that $\mathbb{1} \otimes \Lambda^\dagger(\rho) \not\geq 0$, i.e. we have found a two-decomposable map that detects the state. To prove the converse, let $\Lambda = \Lambda^{CP} \circ T$ be a two-decomposable map such that $\mathbb{1} \otimes \Lambda(\rho)$ has a negative eigenvalue. Denoting by $|\phi\rangle$ the corresponding eigenvector, we get

$$\langle\phi|\mathbb{1} \otimes \Lambda^{CP}(\rho^{T_B})|\phi\rangle = \text{Tr}[(\mathbb{1} \otimes \Lambda^\dagger)(|\phi\rangle\langle\phi|)\rho^{T_B}] < 0. \tag{4.5}$$

It is sufficient to consider $\Lambda^{CP}(A) = VAV^\dagger$, with V a rank-2 operator, therefore $\mathbb{1} \otimes \Lambda^\dagger(|\phi\rangle\langle\phi|) = |\phi'\rangle\langle\phi'|$, with $|\phi'\rangle$ Schmidt rank 2. Thus $\text{Tr}(\rho^{T_B}|\phi'\rangle\langle\phi'|) < 0$, and ρ is 1-distillable. $\square$

When $D = |\psi\rangle\langle\psi|^{T_B}$ the associated map is of the form

$$\rho \rightarrow (\mathbb{1} \otimes V)\rho^{T_B}(\mathbb{1} \otimes V)^\dagger.$$

It is instructive to compare this to Theorem 4.1.2. The above mapping is basically a projection of the partial transposed state on a $\mathbb{C}^n \otimes \mathbb{C}^2$ (this special case was also derived in Ref. [72]). Theorem 4.1.2 characterizes distillability in an analogous manner, but instead projects onto $\mathbb{C}^2 \otimes \mathbb{C}^2$. Thus regarded in this way, the above theorem is both a generalisation and a simplification of the main theorem of distillability.

Note that given a two-decomposable map Λ, the above result implies that undistillable states must satisfy both $(\mathbb{1} \otimes \Lambda)(\rho) \geq 0$ and the dual criterion $(\Lambda \otimes \mathbb{1})(\rho) \geq 0$. As the reader might have guessed, the reduction criterion is just an example of a two-decomposable map, which we will show below. We also give numerous other applications of our Theorem 4.2.1 and Observation 4.2.1, starting with an elementary derivation of some alternative formulations of distillability.

4.2.2   Application 1: Derivation of other distillability theorems

In this section we rederive two distillability theorems. The original derivations were quite lengthy, and as we will show, both theorems follow straightforwardly from our Observation 4.2.1 and some basic theorems on Schmidt numbers from Chapter 2. The following theorem was first derived in Ref. [72], see also the related characterisation in Ref. [257].

Theorem 4.2.2. *Let ρ be a state and S be the completely positive map defined by*

$$\rho = (\mathbb{1} \otimes S)P_+.$$

Let T denote the transpose map. Then ρ is 1-undistillable if and only if $\Lambda = T \circ S$ is two-positive, and more generally n-undistillable if and only if $\Lambda^{\otimes n}$ is two-positive.

Proof. For undistillable states ρ we have that

$$\mathrm{Tr}\,(\rho D) = \mathrm{Tr}\,(\rho^{T_B} D^{T_B}) > 0,$$

for all D^{T_B} having Schmidt number two. From the isomorphism between states positive on Schmidt number k states and k-positive maps (Theorem 2.2.2), we deduce that the map associated with ρ^{T_B} is two-positive for undistillable states. This map is just given by Λ as defined in the statement of the theorem. Thus ρ is 1-undistillable if and only if Λ is two-positive. The second part follows trivially by applying the first part on $\rho^{\otimes n}$ and some elementary algebra. $\square$

The second theorem is a slightly simplified version of the one presented in Ref. [177].

Theorem 4.2.3. *Let P_2 be the projector onto a maximally entangled state acting on $\mathcal{H}_1 = \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1} = \mathbb{C}^2 \otimes \mathbb{C}^2$. Then for an arbitrary operator X acting on $\mathcal{H}_2 = \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$ we can define*

$$W_X = P_2 \otimes X^{T_B}. \tag{4.6}$$

A state ρ acting on $\mathcal{H}_2$ is n-undistillable if and only if $W_{\rho^{\otimes n}}$ is an entanglement witness.

Proof. From Observation 4.2.1 we have that ρ is 1-undistillable if and only if ρ^{T_B} is positive on Schmidt number two states. The theorem then follows directly from Lemma 2.1.2, and from the fact that ρ is n-undistillable if and only if $\rho^{\otimes n}$ is 1-undistillable. $\square$

4.2.3   Application 2: A plethora of reduction-like maps

In this section we show that the map associated with the reduction criterion is two-decomposable, which immediately proves that all states violating the reduction criterion can be distilled. This greatly simplifies the original proof which relied on a series of protocols: filtering, twirling and distillation of isotropic states. Let us construct the operator σ from the Schmidt rank-2 vectors $|\psi_{ij}\rangle = |ij\rangle - |ji\rangle$, $i \neq j$. Adding the corresponding projectors we get

$$\sigma = \sum_{i<j} |\psi_{ij}\rangle\langle\psi_{ij}| = \sum_{i\neq j} (|ij\rangle\langle ij| - |ij\rangle\langle ji|) = \mathbb{1} - F.$$

From this follows that $D = \sigma^{T_B} = \mathbb{1} - dP_+$ is positive on undistillable states. The associated map is given by $\Lambda_1(A) = \text{Tr}(A)\mathbb{1} - A$. This is just the map used by the reduction criterion for entanglement. Thus if a state ρ satisfies $\mathbb{1} \otimes \rho_B - \rho \not\geq 0$ or $\rho_A \otimes \mathbb{1} - \rho \not\geq 0$ then it is 1-distillable. In this way we have also proven that the map is decomposable [131], and using our results one obtains readily the explicit Choi-Kraus form of the map. Next, we construct some other elementary examples by combining different Schmidt rank-2 vectors:

$\diamondsuit$ Taking our vectors $|\psi_{ij}\rangle = |ij\rangle + |ji\rangle$ we obtain

$$\sigma = \sum_{i\neq j} (|ij\rangle\langle ij| + |ij\rangle\langle ji|) = \mathbb{1} + F - 2Z,$$

with $Z = \sum_i |ii\rangle\langle ii|$. Therefore $D = \sigma^{T_B} = \mathbb{1} + dP_+ - 2Z$ and the associated map is given by $\Lambda_2(A) = \text{Tr}\, A\mathbb{1} + A - 2\,\text{diag}\, A$. The map *diag* maps all off-diagonal elements to zero and leaves the diagonal itself invariant.

$\diamondsuit$ For Schmidt rank-2 vectors of the form $|\psi_{ij}\rangle = |ii\rangle + |jj\rangle$, we get:

$$\sigma = \sum_{i\neq j} (|ii\rangle\langle ii| + |ii\rangle\langle jj|) = dP_+ + (d-2)Z,$$

and thus $D = \sigma^{T_B} = F + (d-2)Z$; the associated map is given by $\Lambda_3(A) = A^T + (d-2)\,\text{diag}\, A$.

$\diamondsuit$ If we take Schmidt rank-2 vectors of the form $|\psi_{ij}\rangle = |ii\rangle - |jj\rangle$, we get:

$$\sigma = \sum_{i\neq j} (|ii\rangle\langle ii| - |ii\rangle\langle jj|) = -dP_+ + dZ,$$

and thus $D = \sigma^{T_B} = -F + dZ$; the associated map is given by $\Lambda_4(A) = -A^T + d \operatorname{diag} A$.

$\Diamond$ In fact, *every* operator with Schmidt number 2 gives us a strong distillability witness. In Chapter 2 we have seen that the special isotropic state

$$\sigma = (d-2)\mathbb{1} + (2d-1)dP_+$$

allows a Schmidt rank-2 decomposition. We find $D = \sigma^{T_B} = (d-2)\mathbb{1} + (2d-1)F$ and for the corresponding map $\Lambda_5(A) = (d-2)\operatorname{Tr} A\mathbb{1} + (2d-1)A^T$.

It is worth noting that although these maps are just like the reduction map two-decomposable, they lack any physical interpretation. The reduction criterion on the other hand, has several intuitive properties, linking with other notions in quantum information (see for instance [43, 231]). As an example, note that the hash inequality only gives a non-trivial lower bound on the entanglement of distillation for states violating the reduction criterion [137]. We believe therefore that the presented maps deserve further investigation.

There are however a few general statements we can make about the introduced maps. As we have seen for the separability problem, given an entanglement witness D, the dual positive map Λ will detect much more states (see the discussion after Theorem 1.2.5). In a similar fashion as is shown there, the map Λ corresponds to the class of witnesses $(A \otimes \mathbb{1})D(A^\dagger \otimes \mathbb{1})$, for arbitrary A. It also implies that the criteria $\mathbb{1} \otimes \Lambda(\rho) \geq 0$ and $\Lambda \otimes \mathbb{1}(\rho) \geq 0$ are insensitive to local transformations by one of the parties (thus to filtering operations). Indeed, suppose Alice performs a general measurement, with measurement operators A_1 and A_2 satisfying $A_1^\dagger A_1 + A_2^\dagger A_2 = \mathbb{1}$. Then the state ρ will be transformed into $\rho_i = (A_i \otimes \mathbb{1})\rho(A_i^\dagger \otimes \mathbb{1})/p_i$. It follows that, if the original state did not violate the criteria, then the transformed state does not either. The map corresponds to the operator witness, together with all possible local filtering operations by one of the parties.

We have shown how to construct maps that detect distillability, applicable in arbitrary dimensions, which can be easily evaluated on states. There is however a catch. As can be seen from the reconstruction of the reduction criterion, the witness from which the map is derived, is a convex combination of *many* witnesses. So it is possible that one of those witnesses (and the associated map) detects a state, while the sum does not. In other words, the map could be weaker than expected at first sight. The

sum of the negative eigenvalues of D, or the entanglement of D^{T_B}, can be seen as a measure for the strength of a certain map.

The basic requirement for a distillability witness D to detect a two-distillable state ρ which is not 1-distillable is that D^{T_B} must be entangled with respect to the first and second pair. Indeed suppose $D = |\psi\rangle\langle\psi|^{T_B}$ with $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ separable, then

$$\text{Tr}(D^{T_B}\rho^{\otimes 2 T_B}) = \text{Tr}(|\psi_1\rangle\langle\psi_1|\rho)\,\text{Tr}(|\psi_2\rangle\langle\psi_2|\rho) > 0,$$

since the vectors $|\psi_i\rangle$ have at most Schmidt rank 2. Consider the witness for the reduction criterion on two pairs:

$$D^{T_B} = \mathbb{1} - F = \mathbb{1}_1 \otimes \mathbb{1}_2 - F_1 \otimes F_2.$$

But from Ref. [138] we can write $F = P_S - P_A$ and $\mathbb{1} = P_S + P_A$ with P_S and P_A projection operators onto the symmetric and antisymmetric subspaces respectively. Substitution yields

$$D^{T_B} = P_{S1} \otimes P_{A2} + P_{A1} \otimes P_{S2},$$

so that D^{T_B} is separable with respect to the different pairs. Note that this property is not adhered by the map since $(A \otimes \mathbb{1})D^{T_B}(A^\dagger \otimes \mathbb{1})$ could be entangled with respect to the two pairs, even if D itself is not. So it is not at all obvious that collective application of the reduction criterion (for instance on $\rho^{\otimes 2}$) does not yield a stronger criterion.

It was proven in Ref. [131] that it is not the case, namely, if $\mathbb{1} \otimes \Lambda_1(\rho^{\otimes 2}) \not\geq 0$ then $\mathbb{1} \otimes \Lambda_1(\rho) \not\geq 0$. It is readily verified that all introduced maps share this property. In the case of the reduction criterion, the reverse is also true. This can be proven as follows. From Ref. [131] we have

$$\mathbb{1}_A \otimes \Lambda_B(\rho_1 \otimes \rho_2) = [\mathbb{1}_{A1} \otimes \rho_{B1}] \otimes [\mathbb{1}_{A2} \otimes \Lambda_{B2}](\rho_2) + [\mathbb{1}_{A1} \otimes \Lambda_{B1}](\rho_1) \otimes \rho_2.$$

Now suppose $\mathbb{1} \otimes \Lambda(\rho_i)$ is not a positive operator, so that there exists a vector $|\psi\rangle$ with negative expectation value. From the above expression follows that $\langle\Psi|\mathbb{1}_A \otimes \Lambda_B(\rho_1 \otimes \rho_2)|\Psi\rangle < 0$, with $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. So applying the reduction criterion to one or more pairs is completely equivalent. A similar statement and proof applies for Λ_4, but for the other maps, this reverse statement is not true.

4.2.4 Application 3: Random Schmidt-2 robustness and distillability

The following proposition, first presented in Ref. [61] uses upper bounds to the random Schmidt-2 robustness as defined in Section 2.4.2 to construct a distillability criterion:

Proposition 4.2.1. *Let ρ be an arbitrary bipartite state, such that ρ^{T_B} has negative eigenvalues. Let $|\psi\rangle$ be the eigenvector corresponding to a negative eigenvalue λ and let $\tilde{R}_{r2}(\psi)$ be an upper bound to its random Schmidt-2 robustness. Then ρ is 1-distillable if*

$$\lambda < -\tilde{R}_{r2}(\psi).$$

Proof. From the definition, we have that

$$W = |\psi\rangle\langle\psi| + \tilde{R}_{r2}(\psi)\mathbb{1}$$

has Schmidt number two. Now from Observation 4.2.1 follows that ρ is 1-distillable if $\mathrm{Tr}(W\rho^{T_B}) < 0$. This can we rewritten as

$$\langle\psi|\rho^{T_B}|\psi\rangle + \tilde{R}_{r2}(\psi) = \lambda + \tilde{R}_{r2}(\psi) < 0.$$

$\square$

This proposition provides an important reason to find an exact analytical formula for $R_{r2}(\psi)$. Note that this distillability criterion only depends on the minimum eigenvalue and the corresponding eigenvector. It is easy to see that it is independent of the reduction criterion as we show by means of an example. Consider the state

$$\rho = \frac{1}{16}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & -1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}. \qquad (4.7)$$

It is easy to check that the reduction criterion is not useful here. The partial transposition ρ^{T_B} has an eigenvector $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle - |22\rangle)$ and corresponding eigenvalue $-\frac{1}{8}$. Since $-R_{r2}(\psi) = -\frac{1}{15} > -\frac{1}{8}$, ρ is distillable.

An unconditional distillability criterion, which does only depend on the minimum eigenvalue of ρ^{T_B} would follow from Conjecture 2.4.1. Pending on the proof of this conjecture, we have that ρ is distillable whenever ρ^{T_B} has an eigenvalue $\lambda \leq -1/14$.

4.2.5   Application 4: Volume of 1-distillable states

In this section we will outline a powerful algorithm for the detection of distillable states (first published in Ref. [60]). As before, it is clear that we can confine ourselves to the study of 1-distillability. A first numerical method for this problem was devised by Dür et al. [83] starting from the basic minimisation over Schmidt rank two vectors $|\psi\rangle$:

$$\min_{\psi \in SR2} \langle\psi|\rho^{T_B}|\psi\rangle \overset{?}{<} 0. \tag{4.8}$$

They convert this problem into a minimisation of the minimum eigenvalue of certain matrices. Their method involves also calculating an inverse of a matrix in every step.

In view of our discussion above, we will perform this minimisation not over the distillability witnesses, but over the much stronger associated two-decomposable maps. Thus for a given state ρ, we can reduce the problem (see also again Ref. [72]) to checking whether there exists an operator $P = |0\rangle\langle a| + |1\rangle\langle b|$, with $\langle b|a\rangle = 0$ such that

$$(\mathbb{1} \otimes P)\rho^{T_B}(\mathbb{1} \otimes P)^\dagger \overset{?}{\ngeq} 0.$$

One way of doing this is to parametrize a countable subset of vectors which is dense within all vectors, such as the one introduced in Ref. [159]. Explicitly their set takes the form $G = \{\sum \lambda_i |i\rangle | (\lambda_1, \lambda_2, \cdots, \lambda_d) \in \tilde{G}_\mathbb{N}\}$ with

$$\tilde{G}_N = \left\{ \left(\frac{p_1}{q_1}e^{2\pi i\frac{r_1}{s_1}},, \frac{p_2}{q_2}e^{2\pi i\frac{r_2}{s_2}}, \cdots, \sqrt{1 - \sum_l \frac{p_l^2}{q_l^2}}e^{2\pi i\frac{r_d}{s_d}} \right) \right\}$$

for $0 < p_i \leq q_i \leq N; 0 < r_i \leq s_i \leq N$. Thus for every N, we can construct sets of pairs $|a\rangle$ and $|b\rangle$, and taking N increasingly large we will detect all 1-distillable states, except those arbitrary close to the boundary of the convex set of 1-undistillable states.
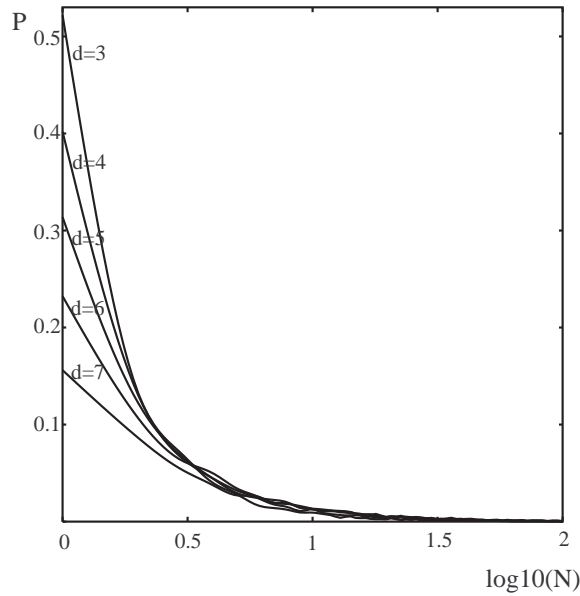
Figure 4.1: The probability of detecting 1-distillability as a function of the test number for random states drawn from $\mathcal{D} \times \mathcal{U}$. For visual purposes only the first 100 tests are depicted and the points have been smoothened out to curves.

In practice two improvements can be made which greatly enhance the performance. First note that the countable subset above will yield vectors $|a\rangle$ and $|b\rangle$ not necessarily orthogonal. Furthermore, clearly such a countable subset will in general not pick vectors uniformly distributed according to the Haar measure. One way of overcoming this is to take for $|a\rangle$ and $|b\rangle$ two columns of a random unitary. Here orthogonality and uniformity are automatically guaranteed. The associated algorithm works well for low dimensional density matrices. For higher dimensions, a local optimisation of the $|a\rangle$ and $|b\rangle$ yielding the minimum after a certain cut-off number of tests turns out to work well. The explicit algorithm has been reproduced in Appendix A.2.

Let us apply this to give a numerical estimate of the volume of 1-distillable states for low dimensional quantum states. A similar numerical estimate has been carried out for entangled states [339, 342]. When talking about volumes on the set of density operators, it is clear that the results will depend on the measure. We choose the measure applied in Ref. [342] as it seems very natural.

A general bipartite quantum state ρ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ can be expanded by virtue

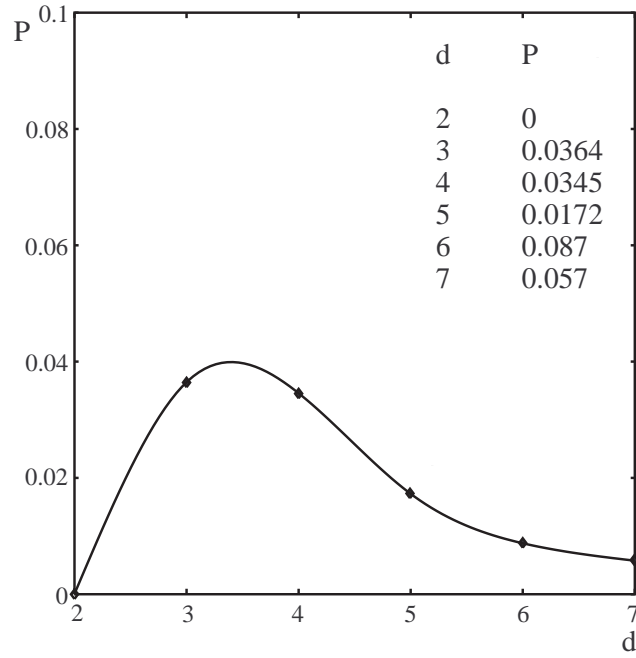| d	P
2	0
3	0.0364
4	0.0345
5	0.0172
6	0.087
7	0.057

Figure 4.2: Probability of a random NPT state drawn from $\mathcal{D} \times \mathcal{U}$ to be 1-undistillable. The curve has been drawn to guide the eye.

of the spectral decomposition as

$$\rho = UDU^\dagger,$$

with $D = (d_{ii})$ diagonal and U unitary. The measure we are going to use is the product measure $\mathcal{D} \times \mathcal{U}$. Here $\mathcal{D}$ represents the uniform distribution of the points on the manifold given by $\sum_i d_{ii} = 1$. A simple method for generating such a distribution from independent uniformly distributed random numbers chosen in the interval $(0, 1)$ is outlined in Appendix A of Ref. [342]. Similarly, $\mathcal{U}$ is chosen to be the uniform measure on unitary matrices (the Haar measure). To generate random unitaries according to this measure one can use the algorithm from Ref. [237, 341] which relies on a decomposition of a general unitary in two-dimensional unitary transformations. A simpler method for generating Haar unitary matrices is as follows [86, 275]. Take a random matrix A, whose entries are complex numbers which are independently normally distributed with mean zero. The polar decomposition $A = PU$, with P positive, then yields U distributed according to $\mathcal{U}$.
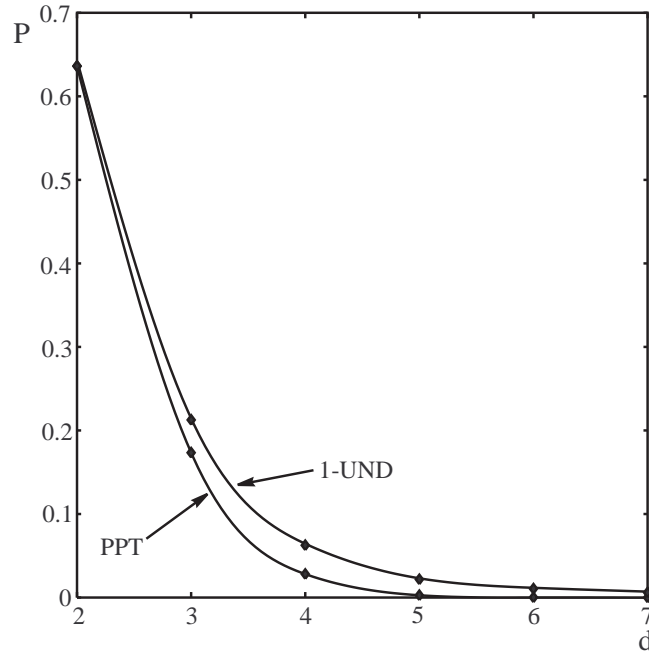
Figure 4.3: Probability of a random state drawn from $\mathcal{D} \times \mathcal{U}$ to be 1-undistillable.

We have tested the our method on 10^5 density matrices acting on $\mathbb{C}^d \otimes \mathbb{C}^d$ for $d = 3, 4, 5, 6, 7$. The estimated probability for proving the distillability of a state as a function of the test number is displayed in Figure 4.1. A striking feature is that the vast majority of the distillable states were detected in the first few tests. This is especially true for low dimensional states. For example for $d = 3$ about half of the NPT states are found to be distillable in the first test. For $d = 7$ the probability of finding a distillable state in the first test is about $1/6$.

In Figure 4.2 the probability of an NPT state being 1-undistillable is plotted versus the dimension d. To obtain sufficient precision we carried out 10^5 random tests per state, and in addition $10^4 d$ optimisation steps seeking for a local minimum. Of course, this method does not guarantee to detect every 1-distillable state, but we obtain an upper bound of the number of undistillable states. The figure suggests that the volume of 1-undistillable states drops to zero for high dimensions. In Figure 4.3 the same graph is drawn, but now PPT states are included.

It is tempting to conclude from this numerical evidence that bound entangled states

are primarily a phenomenon present in low dimensional quantum systems. In high
dimensional systems most undistillable states are therefore situated in the immediate
neighbourhood of the set of separable states. Our results are consistent with the fact
that bound entanglement for continuous variables is a rare phenomenon [152]. In
particular it was shown that the subset of undistillable states is nowhere dense in
the set of bipartite continuous variable states. From this it follows that the set of
undistillable continuous variables states does not contain any open ball, an argument
which was made explicit for separable states in Ref. [92]. Given an infinite dimensional
separable state one can construct sequences of closer and closer states all of which are
entangled. Following the same methods one can explicitly construct a distillable state
in any ϵ-neighbourhood in the trace norm of any state [89]. However, note that in
Ref. [121] a parametrized family of measures on states was introduced, which in some
region yields states primarily 1-undistillable.

4.3   The question of NPT bound entanglement

4.3.1   Early results

As we have seen in Theorem 4.1.4, the question of the existence of NPT bound entangle-
ment is equivalent to the existence of undistillable entangled Werner states. Numerical
evidence seems to suggest that some Werner states are indeed undistillable. However,
the problem is still open, and constitutes one of the major challenges in quantum infor-
mation theory. What has been shown [72, 83] is that there are entangled Werner states
that are n-undistillable for every n, however the range of states for which one is able
to prove this, vanishes as n goes to infinity. We will prove this partial result following
the method presented in Ref. [83]. We start with the following key lemma.

Lemma 4.3.1. *Let P be the projector onto the maximally entangled d-level state and
$Q = \mathbb{1} - P$, then for any Schmidt rank two vector $|\psi\rangle$ we have:*

1. $\langle\psi|\mathbb{1}^{\otimes N-k} \otimes P^{\otimes k}|\psi\rangle \leq \frac{2}{d^k}$

2. $\langle\psi|Q^{\otimes N-k} \otimes P^{\otimes k}|\psi\rangle \leq \frac{2}{d^k}$

3. $\langle\psi|Q^{\otimes N}|\psi\rangle \geq (1 - \frac{2}{d})^N$

Proof. (1) For $k = 1$, this is clearly the case, as the overlap of the maximally entangled state and a Schmidt rank two vector is at most $2/d$ (see Lemma 2.1.1). For $k > 1$ this follows from the case $k = 1$ and $P_d^{\otimes k} = P_{d^k}$.

(2) This follows from $Q \leq \mathbb{1}$.

(3) For $N = 1$, this follows directly from (1) and the definition $Q = \mathbb{1} - P$. We prove it for arbitrary N by induction, so let it be true for a certain $N \geq 1$. Now

$$\langle\psi|Q^{\otimes(N+1)}|\psi\rangle = \text{Tr}[|\psi\rangle\langle\psi|Q \otimes Q^{\otimes N}].$$

Writing this trace as $\text{Tr}(\cdot) = \text{Tr}(\text{Tr}_1(\cdot))$, where we first trace out over the first pair, we get

$$\text{Tr}[|\psi\rangle\langle\psi|Q \otimes Q^{\otimes N}] = \text{Tr}[\text{Tr}_1(|\psi\rangle\langle\psi|Q)Q^{\otimes N}].$$

Now since Q is separable (see (2.1)), it is easy to verify that $\text{Tr}_1(|\psi\rangle\langle\psi|Q)$ can be written as $\sum_i c_i|\psi_i\rangle\psi_i|$ with ψ_i Schmidt rank two. Also from the case $N = 1$ follows that $\text{Tr}[\sum_i c_i|\psi_i\rangle\langle\psi_i|] \geq 1 - 2/d$. $\qquad\qquad\square$

This lemma is practically all we need to present the main result of this section.

Theorem 4.3.1. *The Werner states*

$$\rho = \frac{1}{d^2 + \beta d}(\mathbb{1} + \beta F)$$

with $-1 \leq \beta \leq 1$ are entangled for $\beta < -1/d$ or $-1 \leq \text{Tr}(\rho F) < 0$. They are 1-distillable if and only if $\beta < -1/2$ and n-undistillable for $\beta > -1/d + \epsilon_n$, for some $\epsilon_n > 0$.

Proof. The first part follows from the fact that positivity of the partial transposition is a necessary and sufficient condition for separability of the Werner states [309]. The Werner states are 1-distillable for $\beta < -1/2$, as follows from the overlap of the partial transposition with a Schmidt rank two vector $|\psi\rangle$

$$\langle\psi|\rho^{T_B}|\psi\rangle = 1 + \beta\langle\psi|dP_+|\psi\rangle \geq 1 + 2\beta,$$

where we have used Lemma 2.1.1. For n copies let us put $\alpha = 1 + \beta d$ and $\mathbb{1} = P + Q$ so that

$$\rho^{T_B \otimes n} = Q^{\otimes n} + \alpha R.$$

Here R consists of all the other terms in the tensor product expansion. Note that all these terms contain at least one P. From the previous lemma follows then that for any Schmidt rank two vector $|\psi\rangle$

$$\langle\psi|\rho^{T_B \otimes n}|\psi\rangle \geq (1 - \frac{2}{d})^N + \alpha\langle\psi|R|\psi\rangle.$$

Applying again the previous lemma, we also have that we can calculate a lower bound for $\alpha\langle\psi|R|\psi\rangle$. Thus we can always choose α sufficiently small so that $\langle\psi|\rho^{T_B \otimes n}|\psi\rangle \geq 0$ for which ρ will be n-undistillable. We refer to the original reference and our next section for qualitative results on the value of ϵ_n. $\qquad\square$

From this theorem it was conjectured that all Werner states with $\beta > -1/2$ are undistillable, although $\epsilon_n \to 0$ for $n \to \infty$. Apart from some numerical evidence, the main reason was that at the time these results appeared, not a single example of a state was known which is 2-distillable but 1-undistillable. In the meantime, several such states have appeared [87, 270, 310]. These first examples arose in the context of activation (see Section 4.4). Important progress was made by Watrous [316] who constructed a one-parameter set of distillable states which are n-undistillable in some range. We will discuss these states in the next section. Watrous's result does not seem too unlikely, as the notion of n-distillability, as we explained before, is really as much a mathematical as a physical notion. A distillation process will typically require a very large number of copies, even if the state is 1-distillable.

4.3.2   The UUVVF-invariant states

In this section we will discuss the distillability properties of a certain class of highly symmetric two-parameter states, which includes the Watrous states and two copies of the Werner states, and hence is ideal for the study of distillability. We will see that over a wide range of the parameters, the states are probably undistillable. Other examples of conjectured NPT bound entangled states can be found in Ref. [14].

The set of states we are going to study are the $UUVVF$-invariant states introduced in Section 4.1. A convenient parametrisation of the set of $UUVVF$-invariant states is given by

$$\rho = \mathbb{1}_{12} \otimes \mathbb{1}_{34} + \frac{\epsilon d - 1}{d}(\mathbb{1}_{12} \otimes F_{34} + F_{12} \otimes \mathbb{1}_{34}) + \frac{1 - 2\epsilon d + \delta d^2}{d^2}F_{12} \otimes F_{34}.$$

The set of density operators is restricted by the following inequalities

$$(d-1)^2 + 2\epsilon d(d-1) + \delta d^2 \geq 0,$$

$$d^2 - 1 + 2\epsilon d - \delta d^2 \geq 0,$$

$$(d+1)^2 - 2\epsilon d(d+1) + \delta d^2 \geq 0.$$

This set of states includes the Werner [321] states (2 pairs in $d \otimes d$ for $\delta = \epsilon^2$ and 1 pair in $d^2 \otimes d^2$ for $\epsilon = 1/d$) and the Watrous [316] states ($1 - 2\epsilon d + \delta d^2 = d^2$). The PPT states are just the separable states (see Ref. [309]). The states are entangled for $\epsilon < 0$ or $\delta < 0$ which follows from

$$\rho^{T_B} = Q_{12} \otimes Q_{34} + d\epsilon(P_{12} \otimes Q_{34} + Q_{12} \otimes P_{34}) + \delta d^2 P_{12} \otimes P_{34}, \qquad (4.9)$$

with as usual $Q = \mathbb{1} - P$.

Let us now investigate the distillation properties of these states. To prove distillability, all we need to do is to find Schmidt rank two vectors ψ such that $\langle\psi|\rho^{T_B}|\psi\rangle < 0$. We present three such vectors, which we conjecture to detect all 1-distillable states:

$$|\psi\rangle_A = |00\rangle_{12} \otimes (|00\rangle + |11\rangle)_{34},$$

$$|\psi\rangle_B = |01\rangle_{12} \otimes (|00\rangle + |11\rangle)_{34}, \qquad (4.10)$$

$$|\psi\rangle_C = \sum_{ij} |ii\rangle_A|jj\rangle_B + |i(i+1)\rangle_A|j(j+1)\rangle_B.$$

which detect distillability for the states respectively satisfying

$$d^2 + 3d(\epsilon d - 1) + 2(1 - 2\epsilon d + \delta d^2) < 0,$$

$$\epsilon < \frac{1}{d} - \frac{1}{2},$$

$$\delta < \frac{1}{d^2} - \frac{1}{2}.$$

This set of states is shaded dark grey in Figure 4.4.

Now let us derive results in the other direction, namely which states are undistillable? First let us show that for arbitrary n we can find NPT states which are n-undistillable. We will use the inequalities from Lemma 4.3.1. From (4.9) it follows that all potentially negative terms contain at least one P term. But we will also have a term $\langle\Psi|Q^{\otimes 2N}|\Psi\rangle \geq (1 - \frac{2}{d})^{2N}$, and this term can always dominate when we choose

ϵ and δ small enough. Thus for each n, as long as we choose ϵ *or* δ small enough (but one or both negative), we obtain an n-undistillable NPT state.

Next, let us derive states that are definitely 1-undistillable. From (4.9) and the given inequalities it follows straightforwardly that the states satisfying

$$(1 - 2/d)^2 + \min(4\epsilon, 0) + \min(2\delta, 0) \geq 0,$$

are 1-undistillable. Note that this set does not touch the set of 1-distillable states. The reason for this is that although the inequalities are sharp, the sum of such inequalities are not. In some regions we can get a better bound by rewriting (4.9) as

$$\rho^{T_B} = \mathbb{1}_{12} \otimes \mathbb{1}_{34} + (\epsilon d - 1)(P_{12} \otimes Q_{34} + Q_{12} \otimes P_{34}) + (\delta d^2 - 1)P_{12} \otimes P_{34},$$

and we find that all states such that

$$d^2 + \min(4d(\epsilon d - 1), 0) + \min(2(\delta d^2 - 1), 0) \geq 0$$

are 1-undistillable. This second set of states is depicted in Figure 4.4.

To conclude our discussion of the distillation properties we will discuss the Watrous states [316] of which the general form is given by

$$\rho = \mathbb{1}_{1,2} \otimes \mathbb{1}_{3,4} + \frac{\epsilon d - 1}{d}(\mathbb{1}_{1,2} \otimes F_{3,4} + F_{1,2} \otimes \mathbb{1}_{3,4}) + F_{1,2} \otimes F_{3,4},$$

with $1 + 1/d > \epsilon > 1/d - 1$. The states are entangled if and only if $\epsilon < 0$ and definitely 1-distillable if $\epsilon < 1/d - 1/2$. We will show that all entangled Watrous states are distillable. Suppose now we have two pairs of entangled Watrous states, the second pair having indices $5, 6$ and $7, 8$. Using the identities

$$\mathrm{Tr}((P_{1,5} \otimes P_{2,6})(\mathbb{1}_{1,2} \otimes F_{5,6})) = 1/d,$$

$$\mathrm{Tr}((P_{1,5} \otimes P_{2,6})(F_{1,2} \otimes \mathbb{1}_{5,6})) = 1/d,$$

$$\mathrm{Tr}((P_{1,5} \otimes P_{2,6})(F_{1,2} \otimes F_{5,6})) = 1,$$

it can be verified that projecting upon $P_{1,5} \otimes P_{2,6}$ will yield a new Watrous state ρ' with parameter

$$\epsilon' = \epsilon\left(\frac{2(\epsilon d + d^2 - 1)}{d^2\epsilon^2 + d^2 - 1}\right).$$

Since $\epsilon' < \epsilon$ for $0 > \epsilon > 1/d - 1$, the state will be more entangled than the state we started from for each $\epsilon < 0$. One can repeat this protocol on many pairs until
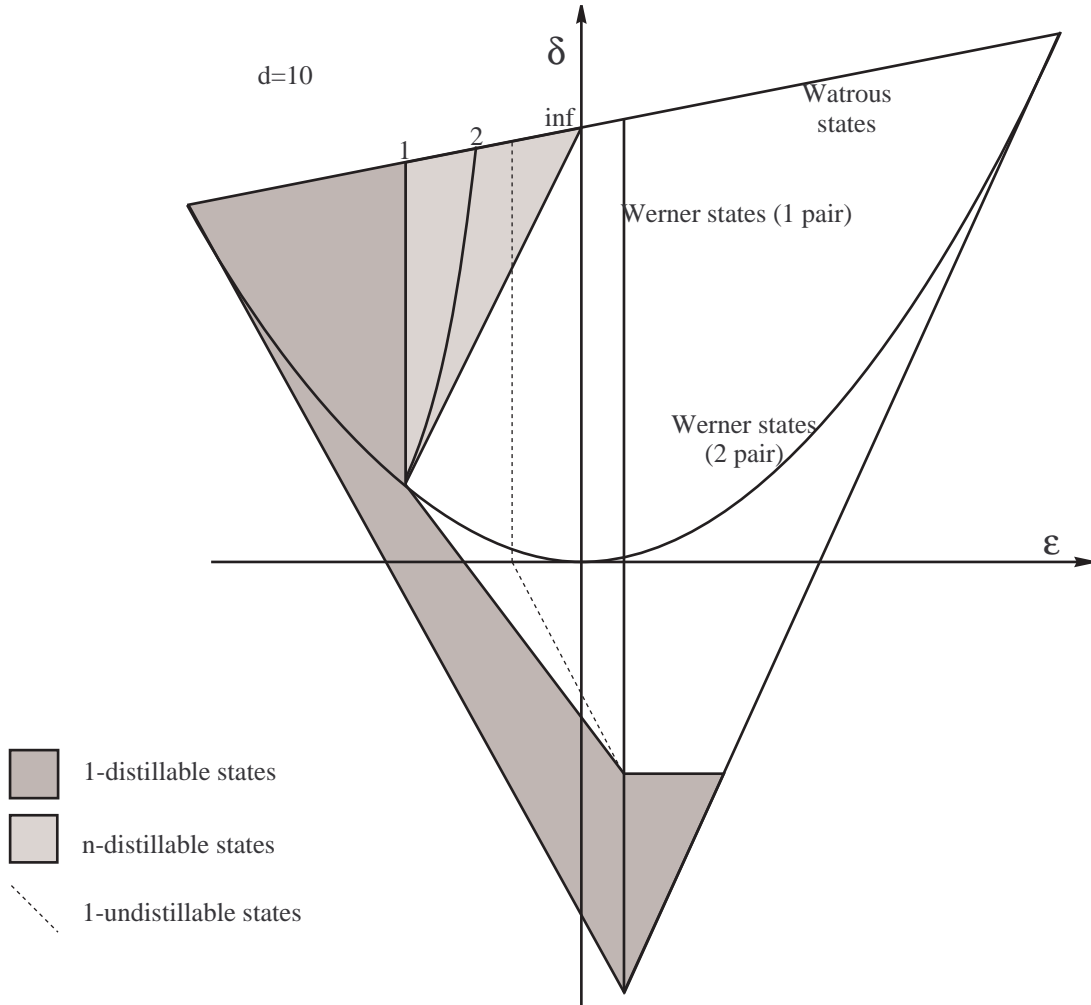
Figure 4.4: $UUVVF$-invariant states. All states satisfying $\epsilon \geq 0$ and $\delta \geq 0$ are separable. Shaded areas mark out distillable states (1,2 and ∞- copy distillable). The states lying above and to the right of the dotted line are states for which we were able to show 1-undistillability.

finally $\epsilon < 1/d - 1/2$, at which point we obtain a 1-distillable state. More generally the protocol can be applied to the whole set of states; a straightforward but tedious calculation leads to

$$\epsilon' = \frac{\epsilon(d^2\delta + d^2 - 1)}{d^2\epsilon^2 + d^2 - 1},$$
$$\delta' = \frac{\epsilon^2(d^2 - 1) + d^2\delta^2}{d^2\epsilon^2 + d^2 - 1}.$$

The states which are 2-distillable with this protocol are depicted in Figure 4.4. Repeating the protocol recursively, it is not hard to show that all states satisfying

$$\delta > \frac{3d^2 + 4d - 8}{2d(d - 2)}\epsilon + 1 - \frac{1}{d^2},$$

are distillable (see again Figure 4.4). In Section 4.2.3 we have seen that the basic requirement for a distillability witness W, to detect 2-distillability of a state ρ (or thus 1-distillability of $\rho^{\otimes 2}$) which is not 1-distillable, is that W^{T_B} be entangled with respect to the two pairs. The Watrous states allow us to illustrate this. Indeed from the above protocol we can deduce that W_2 on $\rho^{\otimes 2}$ will detect 2-distillable states that are not 1-distillable, with

$$W_2 = (P_{15} \otimes P_{26}^T \otimes P_{B,3478})^{T_{2468}}.$$

Here T is the normal transposition, T_{2468} is the transposition with respect to the subsystems $2, 4, 6$ and 8 and P_B is the projector onto $|\psi\rangle_B$ defined in (4.10). The projectors $P_{15} \otimes P_{26}$ are responsible for the entanglement between the first and second pair.

Using the numerically method outlined in Section 4.2.5 we have checked numerically the distillability of the $UUVVF$-invariant states over the complete range of parameters for 1 and 2 copies for $d = 3$. We easily recovered the proposed boundaries for 1-distillability. For two copies, the states act on a $\mathbb{C}^{d^4} \otimes \mathbb{C}^{d^4}$ Hilbert space and numerical matrix manipulations in a space of this magnitude seem very hard. Fortunately, the states are sparse and our method only requires minimisation of the minimum eigenvalue of a $2d^2 \times 2d^2$ matrix. We were able to detect distillability for the Watrous states in $\epsilon > 1/d - 1/2$ readily and exhaustive testing suggest that also the proposed boundary for 2-distillability is correct. This for the first time provides strong evidence that the Werner states are 4-undistillable for $\beta > -1/2$.

4.3.3 As a Schmidt number problem

As we have seen, the NPT bound entangled conjecture is equivalent to the statement that there exists *no* Schmidt rank two vector $|\psi\rangle$ such that

$$\langle \psi | \rho^{T_B \otimes n} | \psi \rangle < 0, \tag{4.11}$$

for all $n \geq 1$ and $\rho^{T_B} = \mathbb{1} - \frac{d}{2}P$. In other words, it seems that affirmation of the conjecture would have to be in the form of an impossibility proof as opposed to a constructive proof. We will reformulate this conjecture in a more tractable form, namely as a special instance of the separability problem, for which a large number of tools are present. As a steppingstone we first show how to translate the distillability problem into the problem of detecting Schmidt number 3. In the next subsection we then reformulate it as a separability problem. We will do so for one, two and n copies of the Werner states.

Let us start with one copy of ρ, for which the answer is known. As ρ belongs to the set of UU-invariant states, ρ^{T_B} will belong to the set of UU^*-invariant states (the isotropic states) and hence will be invariant under the UU^*-twirl: $\mathcal{T}_{UU^*}(\rho^{T_B}) = \rho^{T_B}$. From this follows that

$$\langle \psi | \rho^{T_B} | \psi \rangle = \text{Tr}(P_\psi \rho^{T_B}) = \text{Tr}(\mathcal{T}_{UU^*}(P_\psi)\rho^{T_B}),$$

here $\mathcal{T}_{UU^*}(P_\psi)$ is the operator $P_\psi = |\psi\rangle\langle\psi|$ after application of the UU^*-twirl. Thus we do not need to check over the whole set of Schmidt rank two vectors, but instead over the restricted set of isotropic states with Schmidt number 2. Recall (see (2.1) and Ref. [257, 286]) that if we parametrise the isotropic states as $\rho_\alpha = \mathbb{1} + \alpha P$ then ρ_α has Schmidt number k when

$$\alpha \leq \frac{d(kd-1)}{d-k}.$$

From this follows that $\rho = \mathbb{1} + \beta F$ is 1-distillable if and only if $\text{Tr}(\rho^{T_B}\rho_\alpha) < 0$, with $\alpha = \frac{d(2d-1)}{d-2}$. Going through the algebra we recover that all Werner states ρ_β with $\beta < -1/2$ are 1-distillable.

Let us now look at two copies of the Werner states $\rho^{\otimes 2}$; as pointed out before, these states belong to the larger class of the $UUVVF$-invariant states. Thus the relevant dual set is the set of the UU^*VV^*F-invariant states. For convenience we write the

operators in the order of the indices 1,2,3,4 and omit these indices. With this in mind we parametrise the UU^*VV^*F-invariant states as
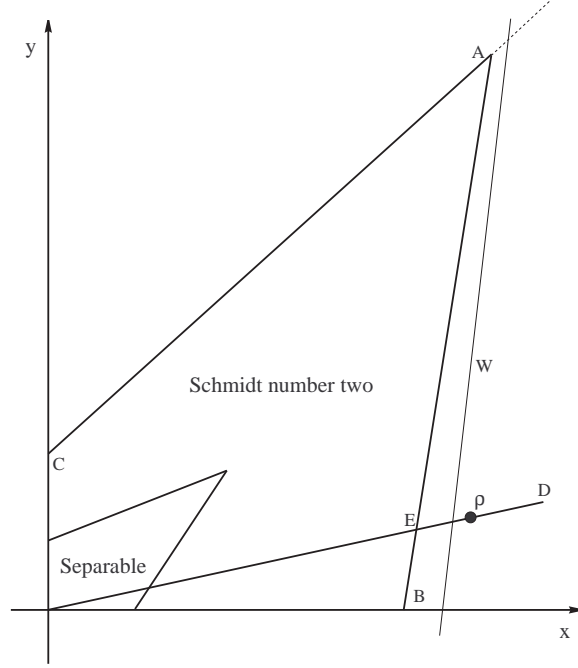
$$\rho = Q \otimes Q + x(Q \otimes P + P \otimes Q) + yP \otimes P,$$

with $x, y > 0$. These states are separable for $d^2 - 2d(x - 1) + (1 - 2x + y) \leq 0$ and $d^2 - (1 - 2x + y) \leq 0$ as depicted in Figure 4.5. The set of Schmidt number 2 states contains at least the convex hull of the points (x, y)

$$A = \left(\frac{(3d - 4)(d + 1)}{2d - 4}, \frac{2(d + 1)^2(d - 1)}{d - 2} \right)$$
$$B = \left(\frac{d^2 - 1}{d - 2}, 0 \right)$$
$$C = \left(0, \frac{2(d^2 - 1)^2}{d^2 - 2} \right)$$

obtained by twirling the Schmidt rank two vectors from equation (4.10). All the states lying above the CA-line have a Schmidt number larger than two. This follows from the fact that the operator $\mathbb{1} \otimes \mathbb{1} - \frac{d^2}{2}P \otimes P$ is positive on Schmidt number 2 states. If the Werner states are 2-undistillable then also all the states lying to the right of the AB-line have Schmidt number at least three. This follows easily by evaluating the expectation value of ρ at $(\mathbb{1} - \frac{d}{2}P)^{\otimes 2}$. Note that it is sufficient to show that all the states ρ on for instance the ED-segment (see Figure 4.5) have Schmidt number 3. This can be seen as follows: let ρ approach E, and suppose we can show that each ρ has Schmidt number 3. This would imply the existence of a hyperplane W separating ρ from the set of Schmidt number 2 states. For ρ arbitrarily close to E this hyperplane would be parallel to the AB-segment, otherwise cutting it. Therefore this would show that all the states lying to the right of the AB-hyperplane have Schmidt number at least three.

For the general case we need to consider the set of $U_1U_1^* \cdots U_nU_n^*F$-invariant states. Here the subindex in U_i refers to the subsystem the unitary operator is acting and the F denotes any permutation of the subsystems. In what follows we will call these states

Figure 4.5: The UU^*VV^*F-invariant states.

$U_iU_i^*F$-invariant states. We parametrise them as

$$\rho = \tilde{Q}^{\otimes n} + x_1(P \otimes \tilde{Q}^{\otimes n-1} + \tilde{Q} \otimes P \otimes \tilde{Q}^{\otimes n-2} + \cdots) +$$
$$x_2(P^{\otimes 2} \otimes \tilde{Q}^{\otimes n-2} + P \otimes \tilde{Q} \otimes P \otimes \tilde{Q}^{\otimes n-2} + \cdots) +$$
$$\cdots + x_n P^{\otimes n},$$

where we have found it convenient to now use the normalised $\tilde{Q} = Q/(d^2 - 1)$. The relevant hyperplane is given by

$$\text{Tr}\left[\left(Q + \left(1 - \frac{d}{2}\right)P\right)^{\otimes n}\rho\right] = 1 + \sum_{i=1}^{n} \binom{n}{i}\left(1 - \frac{d}{2}\right)^i x_i = 0.$$

We can also write this as $1 + \sum_{i=1}^{n} \binom{n}{i}(-1)^i \tilde{x}_i = 0$ with $\tilde{x}_i = \left(\frac{d}{2} - 1\right)^i x_i$. From now on we will continue to work in these normalised variables. Next we will generalise the idea developed for two copies. First we need to show that the hyperplane is spanned by Schmidt number 2 states. Then in order to check distillability, it will be enough to find the boundary between two and three Schmidt number along a line from the origin to an interior point of the points spanning the hyperplane.

An independent set of Schmidt number 2 states spanning the hyperplane is easily obtained as follows (compare to the case for two copies). Let $|\psi\rangle_1 = \frac{1}{\sqrt{2}}|01\rangle^{\otimes n-1} \otimes (|00\rangle + |11\rangle)$. Twirling this state will yield an $U_i U_i^* F$-invariant state with coordinates $(\frac{1}{n}, 0, \cdots, 0)$. Similarly, twirling $|\psi\rangle_2 = \frac{1}{\sqrt{2}}|00\rangle \otimes |01\rangle^{\otimes n-2} \otimes (|00\rangle + |11\rangle)$ will yield an $U_i U_i^* F$-invariant state with coordinates $(\tilde{x}_1 \neq 0, \tilde{x}_2 \neq 0, 0, \cdots, 0)$. In general

$$|\psi\rangle_k = \frac{1}{\sqrt{2}}|00\rangle^{\otimes k} \otimes |01\rangle^{\otimes n-k-1} \otimes (|00\rangle + |11\rangle)$$

will yield a state with coordinates $\tilde{x}_i \neq 0$ for $i \leq k+1$ $\tilde{x}_i = 0$ for $i > k+1$. It is evident that all points will lie on the hyperplane and that they form an independent set, spanning the hyperplane. An interior point can for instance be obtained from the first point, as $(\frac{1}{n} + \epsilon(1 - \frac{1}{n}), \epsilon, \cdots, \epsilon)$ for sufficiently small ϵ. It can readily be verified that this point belongs to the hyperplane by using the identity $\sum_{i=2}^{n} \binom{n}{i}(-1)^i = n - 1$.

Thus n-undistillability of the Werner states beyond the 1-distillability boundary is equivalent to the statement that the $U_i U_i^* F$-invariant state with coordinates $(\frac{1}{n} + \epsilon(1 - \frac{1}{n}) + \delta, \epsilon, \cdots, \epsilon)$ has Schmidt number 3 for $\epsilon > 0$ small enough and all $\delta > 0$.

4.3.4   As a separability problem

In this section we cast the distillability problem as a special instance of the separability problem. Theorem 4.2.3 provides the key ingredient to this, which applied to the conjecture implies that

$$W_X = P_2 \otimes X^{T_B}, \tag{4.12}$$

is an entanglement witness for all $n \geq 1$ with $X = \rho^{\otimes n}$ and $\rho = (\mathbb{1} - F/2)$. We will again use the local symmetry, and present a dual positive formulation of the conjecture. The analysis will be analogous to the reformulation as a Schmidt number problem and a continuous comparison of this section with the previous one is very instructive.

For one pair, we need to prove that $P_2 \otimes (\mathbb{1} - \frac{d}{2}P)$ is an entanglement witness. As before, it will be sufficient to characterize the subset of the separable states of the general $UU^* VV^*$ invariant states. Here U acts on a two-dimensional Hilbert space. We parametrize the $UU^* VV^*$-invariant states as

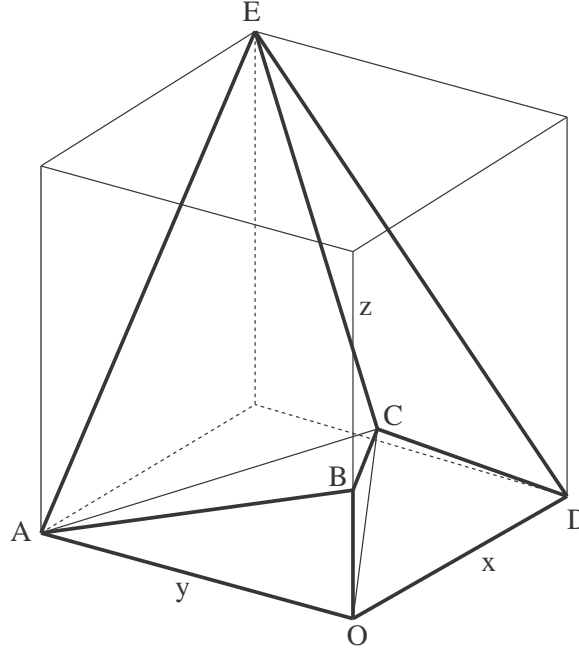$$\rho = \tilde{Q}_2 \otimes \tilde{Q} + xP_2 \otimes \tilde{Q} + y\tilde{Q}_2 \otimes P + zP_2 \otimes P,$$

Figure 4.6: The state space of the UU^*VV^*-invariant states. The point C lies in the xz-plane such that the points A, B, C and E lie in the same plane.

with $x, y, z \geq 0$. The separable states are a subset of the states with positive partial transpose, which satisfy the inequalities

$$3z \leq \frac{1 + 3x}{d - 1} - y \qquad\qquad ABCE\text{-plane}$$

$$z \leq \frac{1 - x}{d + 1} + y \qquad\qquad ECD\text{-plane}$$

$$z \geq \frac{x - 1}{d - 1} + y \qquad\qquad EAD\text{-plane.}$$

Thus the states with positive partial transposition are contained in the polyhedron spanned by the points OABCDE as in Fig 4.6. By twirling the pure separable states $|0101\rangle$, $|0100\rangle$, $|0001\rangle$ and $\sum_{i,j=0}^{1} |ijij\rangle$ one obtains the states represented respectively by the points O, A, C, D and E. Note that B is not in this list. Indeed, as we know that $P_2 \otimes (\mathbb{1} - \frac{d}{2}P)$ is an entanglement witness, all states satisfying $z > 2x/(d-2)$ are entangled. In particular the states in the tetrahedron spanned by the points $ABCO$ are PPT entangled. Conversely, knowing that the polyhedron $ABCO$ is PPT entangled immediately proves that $P_2 \otimes (\mathbb{1} - \frac{d}{2}P)$ is an entanglement witness.

For two copies, we need to consider the $UU^*(V_1V_1^*V_2V_2^*F)$-invariant states which we parametrise as

$$\rho = \tilde{Q}_2 \otimes (\tilde{Q} \otimes \tilde{Q} + y_1(P \otimes \tilde{Q} + \tilde{Q} \otimes P) + y_2 P \otimes P) +$$
$$P_2 \otimes (x_0 \tilde{Q} \otimes \tilde{Q} + x_1(P \otimes \tilde{Q} + \tilde{Q} \otimes P) + x_2 P \otimes P).$$

We will not attempt to completely classify the separable subset, instead it is enough to look at what happens in the neighbourhood of the hyperplane

$$\mathrm{Tr}\left[P_2 \otimes \left(Q + \left(1 - \frac{d}{2}\right)P \right)^{\otimes 2} \rho \right] = x_0 - (d-2)x_1 + \left(\frac{d-2}{2}\right)^2 x_2 = 0.$$

We now show that this hyperplane is spanned by separable states. Consider the following pure separable states and their coordinates $(y_1, y_2, x_0, x_1, x_2)$ after action of the $UU^*(V_1V_1^*V_2V_2^*F)$ twirl:

$$|01\rangle|01\rangle|01\rangle : \quad (0,0,0,0,0)$$

$$|01\rangle|00\rangle|01\rangle : \quad \left(\frac{1}{2(d-1)}, 0, 0, 0, 0 \right)$$

$$|01\rangle|00\rangle|00\rangle : \quad \left(\frac{d-1}{d^2-d-1}, \frac{1}{d^2-d-1}, 0, 0, 0 \right)$$

$$\sum_{i,j=0}^{1} |ij\rangle|ij\rangle|00\rangle : \quad \left(\frac{1}{2(d-1)}, 0, \frac{d-2}{3d}, \frac{3d-4}{6d(d-1)}, \frac{2}{3d(d-1)} \right)$$

$$\sum_{i,j=0}^{1} |ij\rangle|ij\rangle|01\rangle : \quad \left(0, 0, \frac{d-2}{3d}, \frac{1}{3d}, 0 \right).$$

These coordinates can be verified after a tedious but straightforward calculation.

A point in the interior of the convex hull of these points can be obtained by averaging these coordinates. In this case one obtains the state with coordinates $x_0 = 2(d-2)/(15d)$, $x_1 = (5d-6)/(30d(d-1))$, $x_2 = 2/(15d(d-1))$, $y_1 = d(2d-3)/(5(d-1)(d^2-d-1))$ and $y_2 = 1/(5(d^2-d-1))$. From this follows that the Werner states are 2-undistillable if and only if the $UU^*(V_1V_1^*V_2V_2^*F)$-invariant states with coordinates $(y_1, y_2, x_0, x_1 + \epsilon, x_2)$ are entangled for all $\epsilon > 0$.

Let us now move to n copies. The relevant set of states is the set of $UU^*(V_iV_i^*F)$-invariant states

$$\rho = \tilde{Q}_2 \otimes \tilde{Q}^{\otimes n} + \tilde{Q}_2 \otimes [y_1(P \otimes \tilde{Q}^{\otimes n-1} + \tilde{Q} \otimes P \otimes \tilde{Q}^{\otimes n-2} + \cdots) +$$
$$y_2(P^{\otimes 2} \otimes \tilde{Q}^{\otimes n-2} + \cdots) + \cdots + y_n P^{\otimes n-1}] + P_2 \otimes [x_0 \tilde{Q}^{\otimes n} +$$
$$x_1(P \otimes \tilde{Q}^{\otimes n-1} + \tilde{Q} \otimes P \otimes \tilde{Q}^{\otimes n-2} + \cdots) + \cdots + x_n P^{\otimes n}],$$

with $x_i, y_i \geq 0$. The relevant hyperplane is given by

$$\text{Tr}\left[P_2 \otimes \left(Q + \left(1 - \frac{d}{2}\right)P\right)^{\otimes n} \rho\right] = \sum_{i=1}^{n} \binom{n}{i}\left(1 - \frac{d}{2}\right)^i x_i = 0.$$

Renormalising x_i, this can be rewritten as $\sum_{i=1}^{n} \binom{n}{i}(-1)^i \tilde{x}_i = 0$ with $\tilde{x}_i = \left(\frac{d}{2} - 1\right)^i x_i$. Next we will show that this hyperplane touches the set of separable states by constructing a set of $2n + 1$ separable states spanning the hyperplane. The first $n + 1$ states are obtained by twirling

$$|\psi\rangle_k = |01\rangle|00\rangle^{\otimes k}|01\rangle^{\otimes n-k},$$

for $k = 0, \cdots, n$. The twirled state will be $UU^*(V_iV_i^*F)$-invariant and will satisfy $\tilde{x}_i = 0$ for all i and $\tilde{y}_j \neq 0$ for $j \leq k$ and $\tilde{y}_j = 0$ for $j > k$. The last n states are obtained by twirling

$$|\psi\rangle_k = \sum_{i,j=0}^{1} |ij\rangle|ij\rangle|00\rangle^{\otimes n-k-1}|01\rangle^{\otimes k},$$

for $k = 0, \cdots, n - 1$. The twirled state will be $UU^*(V_iV_i^*F)$-invariant and the x coordinates will satisfy $x_j = 0$ for $j > n - k$ and $x_j \neq 0$ for $j \leq n - k$. Therefore the coordinates of the $2n + 1$ states are linearly independent and the choice of $|\psi\rangle_k$ guarantees that the states will lie in the hyperplane.

An interior point in the convex hull of these $2n + 1$ points can be obtained by choosing $\tilde{x}_0 = \epsilon$ and $\tilde{y}_j = \tilde{x}_j = \epsilon$, for ϵ sufficiently small. One verifies that this point belongs to the hyperplane using the identity $\sum_{i=0}^{n-1} \binom{n}{i}(-1)^i = -1$. From this follows that the conjecture is equivalent to the statement that the $UU^*(V_iV_i^*F)$-invariant states with coordinates $\tilde{y}_i = \epsilon$, $\tilde{x}_i = \epsilon$ and $\tilde{x}_1 = \epsilon + \delta$, where $j = 1, \cdots, n$ and $i = 0, 2, \cdots, n$, are entangled for $\epsilon > 0$ small enough and all $\delta > 0$.

Discussion

The general separability problem has been proven to be NP-hard [110]. However, above we showed that the distillability problem can be reformulated as the question of entanglement of a *particular* set of one parameter states. The first and by far still the most elegant tool for detecting entanglement is the partial transposition criterion [222]. However, it is not useful to solve the dual entanglement problem, as it was proven in Ref. [177] that $W_{\rho_W^{\otimes n}}$ is a decomposable entanglement witness if and only if ρ has positive partial transposition. Hence $W_{\rho_W^{\otimes n}}$ will be either a non-decomposable witness or no entanglement witness at all depending on whether $\rho_W^{\otimes n}$ is 1-undistillable or 1-distillable. Thus in order to solve the dual problem, we will either need some powerful tool for detecting PPT-entanglement or a tool for proving separability. However, in the latter case, the original formulation (see (4.11)) seems easier, and for this purpose we presented an efficient algorithm for detecting distillability in Section 4.2.5.

Probably the most powerful method for detecting entanglement is the complete family of separability criteria introduced by Doherty et al. [74, 75], as reviewed in Section 1.2.5. Recall that their method yields an analytical provable entanglement witness from the output of the algorithm. In principle therefore, the distillability problem can be solved for any number of copies, using our dual formulation together with the algorithm associated with the complete family of separability criteria. The numerical method introduced by Eisert et al. [93] can also be employed for this goal. However, note that the reformulation of the distillability problem as a separability problem is unnecessary here, as their method allows for a simple way of checking whether or not an operator is an entanglement witness. Using analogous techniques, it can be extended to testing whether or not an operator is a Schmidt number 3 witness [89]. It should be stressed that the family of criteria introduced by Doherty et al. has the major advantage that an *analytical* canonical entanglement witness can be extracted. Unfortunately, we were unable to test either algorithm, as both methods seem only practical for low dimensional systems. The interesting case, two copies of the Werner states for $d = 3$, could hence not be tested. It would be worth investigating whether these numerical methods could be simplified for the highly symmetrical states we are interested in.

Numerical solutions are one option, another possible approach would be one of a more indirect nature. A powerful method for proving that a certain state is entangled is to show that, when shared by two parties, the state can enhance typical quantum operations such as teleportation or distillation. We will come back to this topic in Section 4.4. One of the main results is [203] that *every* entangled state can enhance the so-called conclusive teleportation fidelity of some other state. This characterisation of entangled states is promising as a way of proving that a certain state is PPT entangled. In Ref. [165] a class of PPT states was constructed which was shown to provide overall convertibility of pure entangled states. In particular it was shown to be able to increase the Schmidt number of a pure state. Now the PPT entangled states we obtained for one copy of the Werner states (tetrahedron ABCO in Figure 4.6) are of a similar form, and although not necessarily in an optimal way, they too can help increase the Schmidt number of a pure state. Similar activation effects can be expected from the conjectured PPT states derived from two copies of the Werner states.

4.3.5   The rainbow states

In this section, as a curiosity, we present a set of states which we conjecture to exhibit all the different forms of distillability. The set of states was inspired by the results of Ref. [165].

The states are $UUVV$-invariant, but with subsystems of unequal dimension (we omit the indices $\{1, 2\}$ and $\{3, 4\}$)

$$\rho = \mathbb{1}_m \otimes \mathbb{1}_d + \frac{d\epsilon - 1}{d}\mathbb{1}_m \otimes F_d + \frac{m\epsilon - 1}{m}F_m \otimes \mathbb{1}_d + \frac{1 - (m + d)\epsilon + dm\delta}{dm}F_m \otimes F_d.$$

In what follows we will assume that $3 \leq m < d$. The set of density operators is restricted by the following inequalities

$$1 + \delta + 2\epsilon + \frac{1}{md} - (\epsilon + 1)\frac{m + d}{md} \geq 0$$

$$1 - \frac{1}{md} + \epsilon\frac{m + d}{md} - \delta + \frac{1}{m} - \frac{1}{d} \geq 0$$

$$1 + \delta - 2\epsilon + \frac{1}{md} + (1 - \epsilon)\frac{m + d}{md} \geq 0$$

The partial transpose is given by

$$\rho^{T_B} = Q_m \otimes Q_d + m\epsilon P_m \otimes Q_d + d\epsilon Q_m \otimes P_d + md\delta P_m \otimes P_d,$$

and it is easy to see that the states are NPT iff $\epsilon < 0$ or $\delta < 0$. Now we will show that these states also include some PPT entangled ones. It is easy to see from equation (2.1.1) in Section 2.1, that $\mathbb{1}_d - dP_d/m$ is positive on Schmidt number m states; it then follows from Lemma 2.1.2 that

$$mP_m \otimes (\mathbb{1}_d - \frac{d}{m}P_d)$$

is an entanglement witness. The partial transpose of an entanglement witness is again an entanglement witness:

$$F_m \otimes (\mathbb{1}_d - \frac{1}{m}F_d).$$

Applying this entanglement witness on ρ we find that the states satisfying

$$\epsilon m^2(d^2 - 1) + dm\delta(m - d) < 0$$

are (PPT) entangled.

Let us now look at the distillation properties. Similar arguments to the ones we used for the $UUVVF$-invariant states apply here. For ϵ or δ sufficiently small, one can find n-undistillable states. The following vectors provide apparently the optimal boundaries for the 1-distillable states (we will only be interested in the states having $\delta > 0$).

1. $|\psi\rangle = |00\rangle_A|00\rangle_B + |10\rangle_A|10\rangle_B$ gives rise to

$$2 + 2(d\epsilon - 1)/d + 4(m\epsilon - 1)/m + 4(1 - (m + d)\epsilon + dm\delta)/(md) < 0$$

2. $|\psi\rangle = |00\rangle_A|01\rangle_B + |10\rangle_A|11\rangle_B$ gives rise to

$$\epsilon < \frac{1}{m} - \frac{1}{2}. \tag{4.13}$$

Now let us take two pairs

$$\rho_1 = \mathbb{1}_m^{34} \otimes \mathbb{1}_d^{12} + \frac{d\epsilon - 1}{d}\mathbb{1}_m^{34} \otimes F_d^{12} + \frac{m\epsilon - 1}{m}F_m^{34} \otimes \mathbb{1}_d^{12} +$$
$$+ \frac{1 - (m + d)\epsilon + dm\delta}{dm}F_m^{34} \otimes F_d^{12},$$

and

$$\rho_2 = \mathbb{1}_m^{78} \otimes \mathbb{1}_d^{56} + \frac{d\epsilon - 1}{d}\mathbb{1}_m^{78} \otimes F_d^{56} + \frac{m\epsilon - 1}{m}F_m^{78} \otimes \mathbb{1}_d^{56} +$$
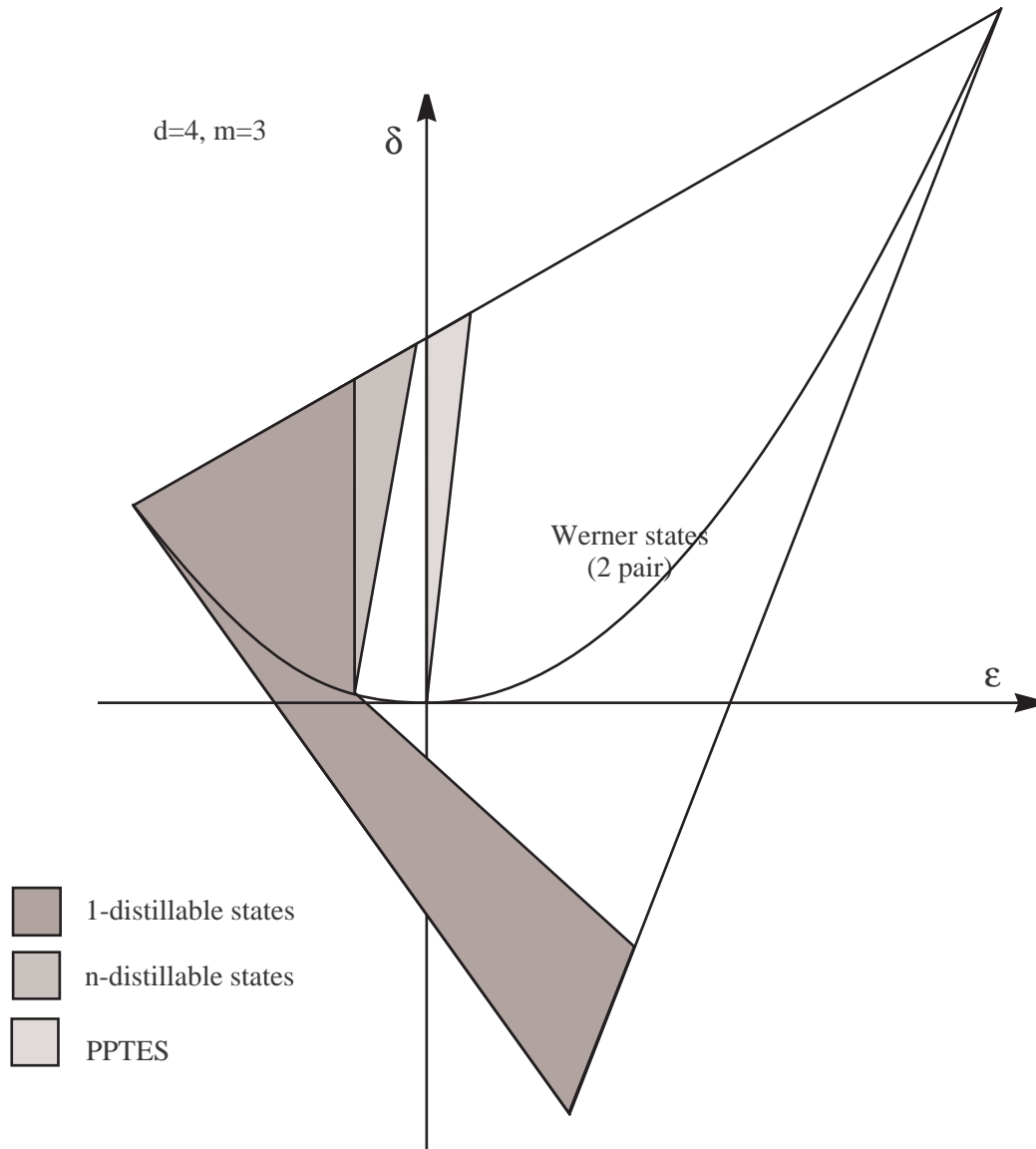$$+ \frac{1 - (m + d)\epsilon + dm\delta}{dm}F_m^{78} \otimes F_d^{56}.$$

Figure 4.7: The rainbow states: the top line of the triangle covers the whole spectrum of different types of distillability.

Taking both pairs together, and projecting upon $P_d^{1,5} \otimes P_d^{2,6}$, we end up with a $UUVVF$-invariant state in $m^2 \otimes m^2$ with

$$\epsilon' = \frac{\epsilon(d^2\delta + d^2 - 1)}{d^2\epsilon^2 + d^2 - 1}$$
$$\delta' = \frac{\epsilon^2(d^2 - 1) + d^2\delta^2}{d^2\epsilon^2 + d^2 - 1}.$$

Now we know when these states can be distilled. The states distillable with this protocol are shown in Figure 4.7. One verifies that projecting upon $P_m^{1,5} \otimes P_m^{2,6}$ performs worse. The set $1 - \frac{1}{md} + \epsilon\frac{m+d}{md} - \delta + \frac{1}{m} - \frac{1}{d} = 0$ contains states of all kinds: 1-distillable, n-undistillable but $n + 1$-distillable, NPT undistillable (conjectured), PPT bound entangled and separable.

4.4   Activation of bound entanglement

As bound entanglement cannot be distilled, it cannot be directly used for typical quantum information tasks, such as teleportation. Activation of bound entanglement is any use of bound entanglement that allows for operations which are not possible by means of LOCC only.

The first of these effects was discovered by the Horodeccy [149]. They showed that a specific state can be quasi-distilled with the aid of an unlimited supply of particular PPT bound entangled states, while this is not possible without them. Although this is a relatively weak result, it was the first indication that bound entanglement can be activated. After this first result, a series of negative results were obtained. Linden and Popescu [188] showed rigorously that some PPT bound entangled state cannot teleport states with better than classical fidelity. Vedral [292] subsequently demonstrated that the PPT distillable entanglement (that is the distillable entanglement of a state in the presence of an unlimited supply of bound entangled states) is still bounded by the relative entropy of entanglement (see also Ref. [73]).

Major progress on activation was made by Shor et al. [270], and their results were later generalised by Eggeling et al. [87]. We discuss this last paper in some detail and sketch the main proofs. Their work is based on the following theorem by Rains [238], which gives a characterisation of the maximal PPT fidelity of distillation F_d.

This quantity is defined as the maximum overlap a state can have with the maximally entangled state P_+ after application of a PPT and trace preserving operation.

Theorem 4.4.1. *The maximal PPT fidelity of distillation of a d-level bipartite state ρ is given by*

$$F_d(\rho) = \max_\Lambda \text{Tr}(P_+ \Lambda(\rho)) = \max_A \text{Tr}(\rho A),$$

where the maximum is taken over all PPT and trace preserving maps Λ or all Hermitian operators A such that $0 \leq A \leq \mathbb{1}$ and $-\mathbb{1} \leq dA^{T_B} \leq \mathbb{1}$.

Proof. (sketch) Since P_+ commutes with all unitaries of the form $U \otimes U^*$ we may assume without loss of generality that $\Lambda(\rho)$ is an isotropic state

$$\Lambda(\rho) = \text{Tr}(\rho B)(\mathbb{1} - P_+) + \text{Tr}(\rho A)P_+,$$

where it is easy to see that the coefficients can always be written as linear functionals on ρ. By the definition of Λ, the operator $\Lambda(\rho)$ has to be a proper quantum state, so we have to require that $0 \leq A, B \leq \mathbb{1}$ and $(d^2 - 1)B + A = \mathbb{1}$. All that is left to do is account for the PPT property of Λ, that is if $\rho > 0$ then

$$\Lambda(\rho^{T_B})^{T_B} = \text{Tr}(\rho B^{T_B})(\mathbb{1} - \frac{F}{d}) + \text{Tr}(\rho A^{T_B})\frac{F}{d} \geq 0.$$

It is easy to see that this is equivalent to $-\mathbb{1} \leq dA^{T_B} \leq \mathbb{1}$.   □

We are now in the position of proving the main result of Eggeling et al. Ref. [87].

Theorem 4.4.2. *With the aid of a bound entangled state any bipartite NPT state is 1-distillable.*

Proof. Denoting P_n the projector onto the negative eigenspace of ρ^{T_B} we define

$$A = \frac{1}{d}(\mathbb{1} - \epsilon P_\text{n}^{T_B}),$$

with $0 < \epsilon \leq \min(2, \|P_\text{n}^{T_B}\|_\infty^{-1})$ and $\| \cdot \|_\infty$ the operator norm (the maximum singular value). It is easy to check that the operator defined in this way meets the conditions of Rains' Theorem. So that

$$\text{Tr}(\rho A) = \frac{1 + \epsilon \mathcal{N}(\rho)}{d},$$

where $\mathcal{N}(\rho) > 0$ is the negativity. Therefore Rains' theorem implies that there exists a PPT and trace preserving operation Λ such that

$$\mathrm{Tr}(\Lambda(\rho)P_+) = \mathrm{Tr}(\rho' P_+) > \frac{1}{d}.$$

and such states are 1-distillable (see Theorem 4.1.3). The proof ends by noting that any PPT preserving map can be implemented locally using a shared PPT bound entangled state (see Section 3.1.3). $\qquad\Box$

An alternative proof using entanglement witnesses can be found in Ref. [177]. It was later also shown that any NPT state can be 1-distilled using only an infinitesimal amount of bound entanglement, as this is possible for the Werner states [310] .

The implications of this result are non-trivial. As pointed out in Ref. [270], it probably implies the superadditivity of the distillable entanglement. Indeed, assuming the existence of NPT bound entanglement we have that there exist states ρ_1 (NPT) and ρ_2 (PPT) such that $E_D(\rho_1) = E_D(\rho_2) = 0$, but

$$E_D(\rho_1 \otimes \rho_2) > 0,$$

where the inequality follows from the previous theorem. This effect is called superactivation, and has been proven to exist in a multipartite setting [271] (see also Ref. [80, 273]). Equally it follows from the existence of NPT bound entanglement that the distillable entanglement is nonconvex, as convexity would imply

$$0 = E_D(\rho_1 \otimes |00\rangle\langle 00|) + E_D(\rho_2 \otimes |11\rangle\langle 11|)$$
$$\geq E_D(\rho_1 \otimes |00\rangle\langle 00| + \rho_2 \otimes |11\rangle\langle 11|) = E_D(\rho) > 0.$$

The last inequality follows from the fact that the states $\rho_1 \otimes |00\rangle\langle 00|$ and $\rho_2 \otimes |11\rangle\langle 11|$ can be locally discriminated. So that when Alice and Bob are given a large number of states ρ they can recover a large supply of ρ_1 and ρ_2, which they can then distill by tensoring them together. In any case, such states ρ are examples of 2-distillable states which are not 1-distillable. In Ref. [130] Michał Horodecki brilliantly argues on why convexity of the distillable entanglement is not to be expected. The argument is based on the fact that the distillable entanglement is a measure characterising the entanglement of source rather than that of individual states (see also [300]).

Another activation effect was demonstrated by Ishizaka [165], who showed that with the aid of specific bound entanglement, pure entanglement is completely interconvertible: all pure entangled states can be converted into each other with some probability, regardless of the Schmidt rank (this was already implicit in Ref. [9]). Theorem 4.4.2 implies that *all* NPT bound entanglement can be activated, as well as some *particular* PPT entangled states. The question remains if every PPT bound entangled state can be activated. Recently, this question was answered affirmatively by Masanes [203]. He showed that any entangled state can enhance the teleportation fidelity of some other state. A special case can be formulated in the context of distillation:

Theorem 4.4.3. *For any entangled state ρ there exists a 1-undistillable state σ such that $\rho \otimes \sigma$ is 1-distillable.*

Although this result is of tremendous importance, the proof works by contradiction, and reveals nothing about the state σ. Not surprisingly, as if this was the case, it would solve the separability problem! A generalisation of this result to multipartite systems was presented in Ref. [204]. Related results were obtained in [34, 297], where it was shown that the generalised robustness (which is nonzero for entangled states) has an operational meaning as the maximum percentual increase an entangled state can provide in the fidelity of teleportation of another state.

Two Matlab programs

A.1 General permutation

The m-file below is a simple implementation of an arbitrary permutation of a density matrix, as defined in (1.12). It is listed here, as some complicated implementations of for instance the partial transpose criterion are circulating. The procedure below is transparent and general. It can also be used to exchange subsystems within a density matrix.

```
function rho2=permcrit(rho,p)
%permcrit(rho,[1 2 4 3]) calculates the partial transposition
%permcrit(rho,[2 4 1 3]) calculates the realigned matrix
%permcrit(rho,[3 4 1 2]) exchanges the first with the second subsystem
%permcrit(rho,[3 5 4 2 6 1]) random permutation for tripartite system
[d1,d2]=size(rho); [s,t]=size(p); n=t/2; d=round(d1^(1/n)); q(p)=1:t;
if s~=1 || floor(t/2)~=ceil(t/2) || ~isequal(q(p),1:t) || length(q)~=t
error('Not a valid permutation'); end;
if d^n~=d1 || d1~=d2, error('Incompatible dimensions'); end;
rho2=zeros(d1,d1); vec=zeros(t,1); dnw=power(d,n-1:-1:0);
for i=0:d1-1, for j=0:d1-1
```

```
 r=1; c=1; i2=i; j2=j;

 for w=1:n, vec(w*2-1)=floor(i2/dnw(w)); vec(w*2)=floor(j2/dnw(w));

 i2=i2-vec(w*2-1)*dnw(w); j2=j2-vec(w*2)*dnw(w); end;

 vec=vec(p);

 for w=1:n, r=r+vec(w*2-1)*dnw(w); c=c+vec(w*2)*dnw(w); end;

 rho2(r,c)=rho(i+1,j+1);

end; end;
```

A.2   Distillability test

The *m*-file below checks whether a state is 1-distillable with the algorithm outlined
in Section 4.2.5. Input parameters are the partial transposed state, the dimension
of the Hilbert spaces of the parties and the number of tests. As the tests involve
randomisation, it is recommended to set the number of tests at least to 10^4, and to
repeat the test a number of times. If the output is negative, however, the state is
guaranteed to be distillable.

```
function mineig=distest(rhotb, d, nrtests)

idxs=zeros(1); mineig=1; precision=-10^(-8);

for yy=1:d

 idxs(2*yy-1)=(yy-1)*d+1; idxs(2*yy)=(yy-1)*d+2;

end;

if issparse(rhotb), EE=sparse(d*d,d*d);

else, EE=zeros(d*d,d*d); end;

for aa=1:nrtests

 [UU,R]=qr(randn(d)+i*randn(d));

 UU=UU*diag(exp(2*pi*i*rand(d,1))); UU(3:d,:)=0;

 for k=1:d:d*d, EE(k:k+d-1,k:k+d-1)=UU; end;

 B=EE*rhotb*EE'; mreig=min(real(eig(full(B(idxs,idxs)))));

 if mreig<mineig, mineig=mreig; UUb=UU; end;

 if mineig<precision, return; end;

end;
```

```
for loop=1:nrtests/d
for counter=1:2
 te1=UUb(counter,:);
 for mn=1:d
 UUb(counter,mn)=randn(1,1)+i*randn(1,1);
 UUb(counter,:)=UUb(counter,:)/norm(UUb(counter,:));
 for k=1:d:d*d, EE(k:k+d-1,k:k+d-1)=UUb; end;
 B=EE*rhotb*EE'; mreig=min(real(eig(full(B(idxs,idxs)))));
 if mreig<mineig, mineig=mreig; te1=UUb(counter,:);
 else, UUb(counter,:)=te1; end;
 end;
 if mineig<precision, return; end;
end; end;
mineig=1;
```

Bibliography

[1] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera. Classification of mixed three-qubit states. *Physical Review Letters*, 87:40401, 2001, quant-ph/0103025.

[2] G. Alber, A. Delgado, N. Gisin, and I. Jex. Efficient bipartite quantum state purification in arbitrary dimensional Hilbert spaces. *Journal of Physics A: Mathematical and General*, 34:8821–8833, 2001, quant-ph/0102035.

[3] A. Ambainis and D. Gottesman. The minimum distance problem for two-way entanglement purification. *IEEE Transactions on Information Theory*, 2004, quant-ph/0310097.

[4] P. Arrighi and C. Patricot. On quantum operations as quantum states. *Annals of Physics*, 311:26–52, 2004, quant-ph/0307024.

[5] H. Aschauer and H. J. Briegel. Quantum communication and decoherence. In *Coherent Evolution in Noisy Environment*. Springer Verlag, 2003.

[6] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49:1804–1807, 1982.

[7] K. Audenaert, J. Eisert, E. Jané, M. B. Plenio, S. Virmani, and B. De Moor. The asymptotic relative entropy of entanglement. *Physical Review Letters*, 87:217902, 2001, quant-ph/0103096.

[8] K. Audenaert, B. De Moor, K. G. H. Vollbrecht, and R. F. Werner. Asymptotic relative entropy of entanglement for orthogonally invariant states. *Physical Review A*, 66:032310, 2002, quant-ph/0204143.

[9] K. Audenaert, M. B. Plenio, and J. Eisert. Entanglement cost under positive-partial-transpose-preserving operations. *Physical Review Letters*, 90:027901, 2003, quant-ph/0207146.

[10] K. M. R. Audenaert and S. L. Braunstein. On strong superadditivity of the entanglement of formation. *Communications in Mathematical Physics*, 246:443–452, 2003, quant-ph/0303045.

[11] R. Augusiak and P. Horodecki. Bound entanglement can maximally violate Bell inequalities: quantum entanglement is not equivalent to quantum security. 2004, quant-ph/0405187.

[12] P. Badziąg, M. Horodecki, A. Sen(De), and U. Sen. Locally accessible information: How much can the parties gain by cooperating. *Physical Review Letters*, 91: 117901, 2003, quant-ph/0304040.

[13] S. Bandyopadhyay. Qubit and entanglement assisted optimal entanglement concentration. *Physical Review A*, 62:032308, 2000, quant-ph/9911013.

[14] S. Bandyopadhyay and V. Roychowdhury. Maximally-disordered distillable quantum states. *Physical Review A*, 69:040302(R), 2004, quant-ph/0302043.

[15] S. Bandyopadhyay, S. Ghosh, and V. Roychowdhury. Non-full rank bound entangled states satisfying the range criterion. *Physical Review A*, 71:012316, 2005, quant-ph/0406023.

[16] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195–200, 1964.

[17] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38:447–452, 1966.

[18] F. Benatti, R. Floreanini, and M. Piani. Non-decomposable quantum dynamical semigroups and bound entangled states. *Open Systems and Information Dynamics*, 11:325–338, 2004, quant-ph/0411095.

[19] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53:2046–2052, 1996, quant-ph/9511030.

[20] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76:722–725, 1996, quant-ph/9511027.

[21] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996, quant-ph/9604024.

[22] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59:1070–1091, 1999, quant-ph/9804053.

[23] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases and bound entanglement. *Physical Review Letters*, 82:5385, 1999, quant-ph/9808030.

[24] R. A. Bertlmann, H. Narnhofer, and W. Thirring. Geometric picture of entanglement and Bell inequalities. *Physical Review A*, 66:032319, 2002, quant-ph/0111116.

[25] R. Bhatia. *Matrix Analysis*. Springer Verlag, New York, 1997.

[26] D. Bohm. *Quantum theory*. Prentice-Hall, New York, 1951.

[27] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 48:696–702, 1935.

[28] H. Bombin and M. A. Martin-Delgado. Entanglement distillation protocols and number theory. *Physical Review A*, 72:032313, 2005, quant-ph/0503013.

[29] S. Bose, V. Vedral, and P. L. Knight. Multiparticle generalization of entanglement swapping. *Physical Review A*, 57:822–829, 1998, quant-ph/9708004.

[30] S. Bose, V. Vedral, and P. L. Knight. Purification via entanglement swapping and conserved entanglement. *Physical Review A*, 60:194–197, 1999, quant-ph/9812013.

[31] M. Bourennane, M. Eibl, C. Kurtsiefer, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera. Witnessing multipartite entanglement. *Physical Review Letters*, 92:087902, 2004, quant-ph/0309043.

[32] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[33] F. G. S. L. Brandão. Quantifying entanglement with witness operators. *Physical Review A*, 72:022310, 2005, quant-ph/0503152.

[34] F. G. S. L. Brandão. Quantifying the activation power of bipartite entangled states. 2005, quant-ph/0510078.

[35] F. G. S. L. Brandão and R. O. Vianna. Witnessed entanglement. *International Journal of Quantum Information*, 4:331–340, 2006, quant-ph/0405096.

[36] H.-P. Breuer. An optimal entanglement criterion for mixed quantum states. *Physical Review Letters*, 97:080501, 2006, quant-ph/0605036.

[37] D. Bruß. Characterizing entanglement. *Journal of Mathematical Physics*, 43: 4237–4251, 2002, quant-ph/011078.

[38] D. Bruß and A. Peres. Construction of quantum states with bound entanglement. *Physical Review A*, 61:30301, 2000, quant-ph/9911056.

[39] D. Bruß, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera. Reflections upon separability and distillability. *Journal of Modern Optics*, 49:1399–1418, 2002, quant-ph/0110081.

[40] H. A. Carteret, A. Higuchi, and A. Sudbery. Multipartite generalisation of the schmidt decomposition. *Journal of Mathematical Physics*, 41:7932–7939, 2000, quant-ph/0006125.

[41] D. Cavalcanti. Connecting the generalized robustness and the geometric measure of entanglement. *Physical Review A*, 73:044302, 2006, quant-ph/0602031.

[42] L.X. Cen, N.-J. Wu, F.-H. Yang, and J.-H. An. Local transformation of mixed states of two qubits to Bell diagonal states. *Physical Review A*, 65:052318, 2002, quant-ph/0203092.

[43] N. J. Cerf, C. Adami, and R. M. Gingrich. Reduction criterion for separability. *Physical Review A*, 60:898–909, 1997, quant-ph/9710001.

[44] K. Chen and L. A. Wu. A matrix realignment method for recognizing entanglement. *Quantum Information and Computation*, 3:193–202, 2003, quant-ph/0205017.

[45] K. Chen and L. A. Wu. The generalized partial transposition criterion for separability of multipartite quantum states. *Physics Letters A*, 306:14–20, 2002, quant-ph/0208058.

[46] K. Chen, S. Albeverio, and S.-M. Fei. Entanglement of formation of bipartite quantum states. *Physical Review Letters*, 95:210501, 2005, quant-ph/0511155.

[47] Y. X. Chen and D. Yang. The relative entropy of entanglement of Schmidt correlated states and distillation. 2002, quant-ph/0204152.

[48] Y.-X. Chen, J.-S Jin, and D. Yang. Distillation of multiple copies of Bell states. *Physical Review A*, 67:014302, 2003, quant-ph/0204004.

[49] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10:285–290, 1975.

[50] M.-D. Choi. Positive semidefinite biquadratic forms. *Linear Algebra and its Applications*, 12:95–100, 1975.

[51] M.-D. Choi. Extremal positive semidefinite forms. *Mathematische Annalen*, pages 1–18, 1977.

[52] M.-D. Choi. Some assorted inequalities for positive linear maps on C^*-algebras. *Journal of Operator Theory*, 4:271–285, 1980.

[53] M.-D. Choi. Positive linear maps. *Proceedings of Symposia in Pure Mathematics*, 38:583–589, 1982.

[54] M. Christandl. *The structure of bipartite quantum states: Insights from group theory and cryptography*. PhD thesis, University of Cambridge, 2006.

[55] M. Christandl and A. Winter. Squached entanglement – An additive entanglement measure. *Journal of Mathematical Physics*, 45:829–840, 2004, quant-ph/0308088.

[56] D. Chruściński and A. Kossakowski. On the structure of entanglement witnesses and new class of positive indecomposable maps. 2006, quant-ph/0606211.

[57] J. I. Cirac. Private communication, 2004.

[58] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein. Entangling operations and their implementation using a small amount of entanglement. *Physical Review Letters*, 86:544–547, 2001, quant-ph/0007057.

[59] L. Clarisse. Characterization of distillability of entanglement in terms of positive maps. *Physical Review A*, 71:032332, 2005, quant-ph/0403073.

[60] L. Clarisse. The distillability problem revisited. *Quantum Information and Computation*, 6:539–560, 2006, quant-ph/0510035.

[61] L. Clarisse. On the Schmidt robustness of pure states. *Journal of Physics A: Mathematical and General*, 39:4239–4249, 2006, quant-ph/0512012.

[62] L. Clarisse. Construction of bound entangled edge states with special ranks. *Physics Letters A*, 2006, quant-ph/0603283.

[63] L. Clarisse and P. Wocjan. On independent permutation separability criteria. *Quantum Information and Computation*, 6:277–288, 2005, quant-ph/0504160.

[64] L. Clarisse, S. Ghosh, S. Severini, and A. Sudbery. Entangling power of permutations. *Physical Review A*, 72:012314, 2005, quant-ph/0502040.

[65] J. F. Clauser and A. Shimony. Bell's theorem: experimental tests and implications. *Reports of Progress in Physics*, 41:1881–1927, 1978.

[66] J. F. Clauser, A. M. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[67] J. de Pillis. Linear transformations which preserve hermitian and positive semidefinite operators. *Pacific Journal of Mathematics*, 23:129–137, 1967.

[68] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete. Local permutations of products of Bell states and entanglement distillation. *Physical Review A*, 67: 022310, 2003, quant-ph/0207154.

[69] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical Review Letters*, 77:2818–2821, 1996, quant-ph/9604039.

[70] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society London A*, 461:207–235, 2005, quant-ph/0306078.

[71] D. P. DiVincenzo and B. M. Terhal. Product bases in quantum information theory. In A. Fokas, A. Grigoryan, T. Kibble, and B. Zegarlinski, editors, *13th International Congress of Mathematical Physics*, pages 399–407. International Press, Boston, 2002.

[72] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal. Evidence for bound entangled states with negative partial transpose. *Physical Review A*, 61:062312, 2000, quant-ph/9910026.

[73] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases, uncompletable product bases and bound entanglement. *Communications in Mathematical Physics*, 238:379–410, 2003, quant-ph/9908070.

[74] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88:187904, 2002, quant-ph/0112007.

[75] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69:022308, 2004, quant-ph/0308032.

[76] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Detecting multipartite entanglement. *Physical Review A*, 71:032333, 2005, quant-ph/0407143.

[77] M. J. Donald, M. Horodecki, and O. Rudolph. The uniqueness theorem for entanglement measures. 2001, quant-ph/0105017v1.

[78] M. J. Donald, M. Horodecki, and O. Rudolph. The uniqueness theorem for entanglement measures. *Journal of Mathematical Physics*, 43:4252–4272, 2002, quant-ph/0105017.

[79] W. Dür. Multipartite bound entangled states that violate Bell's inequality. *Physical Review Letters*, 87:230402, 2001, quant-ph/0107050.

[80] W. Dür and J. I. Cirac. Activating bound entanglement in multi–particle systems. *Physical Review A*, 62:022302, 2000, quant-ph/0002028.

[81] W. Dür and J. I. Cirac. Nonlocal operations: purification, storage, compression, tomography, and probabilistic implementation. *Physical Review A*, 64:012317, 2001, quant-ph/0012148.

[82] W. Dür and J. I. Cirac. Classification of multi–qubit mixed states: separability and distillability properties. *Physical Review A*, 61:042314, 2000, quant-ph/9911044.

[83] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß. Distillability and partial transposition in bipartite systems. *Physical Review A*, 61:062313, 2000, quant-ph/9910022.

[84] K. Eckert and H. Kreutzmann. Quantum-information-theory wintersemester 2000/2001. http://lodda.iqo.uni-hannover.de/, 2002.

[85] K. Eckert, O. Gühne, F. Hulpke, P. Hyllus, J. Korbicz, J. Mompart, D. Bruß, M. Lewenstein, and A. Sanpera. Entanglement properties of composite quantum systems. In T. Beth and G. Leuchs, editors, *Quantum Information Processing*, chapter 7, pages 83–99. Wiley, 2005.

[86] A. Edelman and N. R. Rao. Random matrix theory. *Acta Numerica*, 14:1–65, 2005.

[87] T. Eggeling, K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf. Distillability via protocols respecting the positivity of partial transpose. *Physical Review Letters*, 87:257902, 2001, quant-ph/0104095.

[88] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[89] J. Eisert. Private communication, 2005-2006.

[90] J. Eisert and H. J. Briegel. The Schmidt measure as a tool for quantifying multi-particle entanglement. *Physical Review A*, 64:022306, 2001, quant-ph/0007081.

[91] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilkens. Classical information and distillable entanglement. *Physical Review Letters*, 84:1611–1614, 2000, quant-ph/9907021.

[92] J. Eisert, C. Simon, and M. B. Plenio. On the quantification of entanglement in infinite dimensional quantum systems. *Journal of Physics A*, 35:3911–3923, 2002, quant-ph/0112064.

[93] J. Eisert, P. Hyllus, O. Gühne, and M. Curty. Complete hierarchies of efficient approximations to problems in entanglement theory. *Physical Review A*, 70:062317, 2005, quant-ph/0407135.

[94] A. Ekert and P. L. Knight. Entangled quantum systems and the Schmidt decomposition. *American Journal of Physics*, 63:415–423, 1995.

[95] M.-H. Eom and S.-H. Kye. Duality for positive linear maps in matrix algebras. *Mathematica Scandinavia*, 80:130–142, 2000.

[96] H. Fan. A note on separability criteria for multipartite state. 2002, quant-ph/0210168.

[97] S.-M. Fei, X. Li-Jost, and B.-Z. Sun. A class of bound entangled states. *Physics Letters A*, 352:321–325, 2006, quant-ph/0603105.

[98] J. D. Franson. Bell inequality for position and time. *Physical Review Letters*, 62: 2205–2208, 1989.

[99] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28:938–941, 1972.

[100] E. S. Fry and T. Walther. Atom based tests of the Bell inequalities: the legacy of John Bell continues. In R.A. Bertlmann and A. Zeilinger, editors, *Quantum [Un]speakables*, pages 103–117. Springer, Berlin-Heidelberg-New York, 2002.

[101] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen. Distinguishability of the Bell states. *Physical Review Letters*, 87:277902, 2001, quant-ph/0106148.

[102] S. Ghosh, G. Kar, and A. Roy. Local cloning of Bell states and distillable entanglement. *Physical Review A*, 69:052312, 2004, quant-ph/0311062.

[103] S. Ghosh, P. Joag, G. Kar, S. Kunkri, and A. Roy. Locally accessible information and distillation of entanglement. *Physical Review A*, 71:012321, 2005, quant-ph/0403134.

[104] N. Gisin. Bell inequality holds for all non-product states. *Physics Letters A*, 154: 201–202, 1991.

[105] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Physics Letters A*, 210:151–156, 1996.

[106] A. M. Gleason. Measures on the closed subspaces of a Hilbert space. *Journal of Mathematics and Mechanics*, 6(6):885–893, 1957.

[107] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. Detection of entanglement with few local measurements. *Physical Review A*, 66:062305, 2002, quant-ph/0205089.

[108] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera. Experimental detection of entanglement via witness operators and local measurements. *Physical Review A*, 66:62305, 2002, quant-ph/0210134.

[109] O. Gühne, M. Mechler, G. Tóth, and P. Adam. Entanglement criteria based on local uncertainty relations are strictly stronger than the computable cross norm criterion. *Physical Review A*, 74:010301(R), 2006, quant-ph/0604050.

[110] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the 35th ACM Symposium on Theory of Computing*, pages 10–19, New York, 2003.

[111] K.-C. Ha. A class of atomic positive linear maps in matrix algebras. *Linear Algebra and its Applications*, 359:277–290, 2003.

[112] K.-C. Ha and S.-H. Kye. Construction of entangled states with positive partial transposes based on indecomposable positive linear maps. *Physics Letters A*, 325: 315–324, 2004, quant-ph/0310109.

[113] K.-C. Ha and S.-H. Kye. Construction of $3 \otimes 3$ entangled edge states with positive partial transposes. *Journal of Physics A: Mathematical and General*, 38:9039–9050, 2005, quant-ph/0509079.

[114] K.-C. Ha, S.-H. Kye, and Y. S. Park. Entangled states with positive partial transposes arising from indecomposable positive linear maps. *Physics Letters A*, 313:163–174, 2003, quant-ph/0305005.

[115] W. Hall. Constructions of indecomposable positive maps based on a new criterion of indecomposability. 2006, quant-ph/0607035.

[116] L. Hardy. A method of areas for manipulating the entanglement properties of one copy of a two-particle pure state. *Physical Review A*, 60:1912–1923, 1999, quant-ph/9903001.

[117] A. W. Harrow and M. A. Nielsen. How robust is a quantum gate in the presence of noise. *Physical Review A*, 68:012308, 2003, quant-ph/0301108.

[118] M. Hayashi. General formulas for fixed-length quantum entanglement concentration. *IEEE Transactions on Information Theory*, 52:1904–1921, 2006, quant-ph/0206187.

[119] M. Hayashi and K. Matsumoto. Variable length universal entanglement concentration by local operations and its application to teleportation and dense coding. 2001, quant-ph/0109028.

[120] M. Hayashi, M. Koashi, K. Matsumoto, F. Morikoshi, and A. Winter. Error exponents for entanglement concentration. *Journal of Physics A: Mathematical and General*, 36:36 527–553, 2003, quant-ph/0206097.

[121] P. Hayden, D. W. Leung, and A. Winter. Aspects of generic entanglement. *Communications in Mathematical Physics*, 265:95–117, 2006, quant-ph/0407049.

[122] P. M. Hayden, M. Horodecki, and B. M. Terhal. The asymptotic entanglement cost of preparing a quantum state. *Journal of Physics A: Mathematical and General*, 34:6891–6898, 2001, quant-ph/0008134.

[123] L. Henderson and V. Vedral. Information, relative entropy of entanglement and irreversibility. *Physical Review Letters*, 84:2263–2267, 2000, quant-ph/9909011.

[124] R. D. Hill. Linear transformations which preserve Hermitian matrices. *Linear Algebra and its Applications*, 6:257–262, 1973.

[125] T. Hiroshima and M. Hayashi. Finding a maximally correlated state - Simultaneous Schmidt decomposition of bipartite pure states. *Physical Review A*, 70: 030302(R), 2004, quant-ph/0405107.

[126] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, Cambridge, United Kingdom, 1985.

[127] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, 1991.

[128] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94:160502, 2005, quant-ph/0309110.

[129] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki. Low dimensional bound entanglement with one-way distillable cryptographic key. 2005, quant-ph/0506203.

[130] M. Horodecki. Entanglement measures. *Quantum Information and Computation*, 1:3–26, 2001.

[131] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59:4206–4216, 1999, quant-ph/9708015.

[132] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1–8, 1996, quant-ph/9605038.

[133] M. Horodecki, P. Horodecki, and R. Horodecki. Inseparable two spin-$\frac{1}{2}$ density matrices can be distilled to a singlet form. *Physical Review Letters*, 78:574–577, 1997, quant-ph/9607009.

[134] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a 'bound' entanglement in nature? *Physical Review Letters*, 80:5239–5242, 1998, quant-ph/9801069.

[135] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *Physical Review Letters*, 84:2014–2017, 1999, quant-ph/9908065.

[136] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction and quasi-distillation. *Physical Review A*, 60:1888–1898, 1999, quant-ph/9807091.

[137] M. Horodecki, P. Horodecki, and R. Horodecki. Unified approach to quantum capacities: towards quantum noisy coding theorem. *Physical Review Letters*, 85: 433–436, 2000, quant-ph/0003040.

[138] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and quantum communication. In *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*. Springer, 2001.

[139] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps. *Physics Letters A*, 283:1–7, 2001, quant-ph/0006071.

[140] M. Horodecki, A. Sen(De), and U. Sen. Rates of asymptotic entanglement transformations for bipartite mixed states: Maximally entangled states are not special. *Physical Review A*, 67:062314, 2003, quant-ph/0207031.

[141] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki. Local indistinguishability: more nonlocality with less entanglement. *Physical Review Letters*, 90:047902, 2003, quant-ph/0301106.

[142] M. Horodecki, P. W. Shor, and M. B. Ruskai. General entanglement breaking channels. *Reviews of Mathematical Physics*, 15:629–641, 2003, quant-ph/0302031.

[143] M. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen. Distillation protocols: output entanglement and local mutual information. *Physical Review Letters*, 93: 170503, 2004, quant-ph/0405185.

[144] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed quantum states: Linear contractions and permutation criteria. *Open Systems and Information Dynamics*, 13:103–111, 2006, quant-ph/0206008.

[145] P. Horodecki. Direct estimation of elements of quantum states algebra and entanglement detection via linear contractions. *Physics Letters A*, 319:1–7, 2003.

[146] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232:333–339, 1997, quant-ph/9703004.

[147] P. Horodecki and M. Demianowicz. Unconditional fidelity thresholds in single copy distillation and some aspects of quantum error correction. 2005, quant-ph/0501105.

[148] P. Horodecki and M. Lewenstein. Bound entanglement and continuous variables. *Physical Review Letters*, 85:2657–2660, 2000, quant-ph/0001035.

[149] P. Horodecki, M. Horodecki, and R. Horodecki. Bound entanglement can be activated. *Physical Review Letters*, 82:1056–1059, 1998, quant-ph/9806058.

[150] P. Horodecki, R. Horodecki, and M. Horodecki. Entanglement and thermodynamical analogies. *Acta Physica Slovacia*, 48:141–156, 1998, quant-ph/9805072.

[151] P. Horodecki, M. Lewenstein, G. Vidal, and I. Cirac. Operational criterion and constructive checks for the separability of low rank density matrices. *Physical Review A*, 62:032310, 2000, quant-ph/0002089.

[152] P. Horodecki, J. I. Cirac, and M. Lewenstein. Bound entanglement for continuous variables is a rare phenomenon. In S. L. Braunstein and A. K. Pati, editors, *Quantum Information with Continuous Variables*, pages 211–230. Springer, 2003.

[153] P. Horodecki, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal. Rank two bipartite bound entangled states do not exist. *Theoretical Computer Science*, 293:589–596, 2003, quant-ph/9910122.

[154] R. Horodecki, M. Horodecki, and P. Horodecki. Teleportation, Bell's inequalities and inseparability. *Physics Letters A*, 222:21–25, 1996, quant-ph/9606027.

[155] E. Hostens, J. Dehaene, and B. De Moor. The equivalence of two approaches to the design of entanglement distillation protocols. 2004, quant-ph/0406017.

[156] E. Hostens, J. Dehaene, and B. De Moor. Asymptotic adaptive bipartite entanglement distillation protocol. *Physical Review A*, 73:062337, 2006, quant-ph/0602205.

[157] J.-Y. Hsieh, C.-M. Li, and D.-S. Chuu. A simplification of entanglement purification. *Physics Letters A*, 328:94–101, 2004, quant-ph/0304069.

[158] L.-Y. Hsu. Optimal entanglement purification via entanglement swapping with least classical communication. *Physics Letters A*, 297:126–128, 2002.

[159] F. Hulpke and D. Bruß. A two-way algorithm for the entanglement problem. *Journal of Physics A: Mathematical and General*, 38:5573–5579, 2005, quant-ph/0407179.

[160] F. Hulpke, D. Bruß, M. Lewenstein, and A. Sanpera. Simplifying Schmidt number witnesses via higher-dimensional embeddings. *Quantum Information and Computation*, 4:207–221, 2004, quant-ph/0401118.

[161] P. Hyllus, O. Gühne, D. Bruß, and M. Lewenstein. Relations between entanglement witnesses and Bell inequalities. *Physical Review A*, 72:012321, 2005, quant-ph/0504079.

[162] L. M. Ioannou. Deterministic computational complexity of the quantum separability problem. 2006, quant-ph/0603199.

[163] C. J. Isham. *Lectures on Quantum Theory: Mathematical and Structural Foundations.* Imperial College Press, London, 1995.

[164] S. Ishizaka. Binegativity and geometry of entangled states in two qubits. *Physical Review A*, 69:020301(R), 2004, quant-ph/0308056.

[165] S. Ishizaka. Bound entangled states provide overall convertibility of pure entangled states. *Physical Review Letters*, 93:190501, 2004, quant-ph/0403016.

[166] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.

[167] M. Jammer. *The conceptual development of quantum mechanics. The interpretation of quantum mechanics in historical perspective.* John Wiley, 1974.

[168] E. Jané. Purification of two-qubit mixed states. *Quantum Information and Computation*, 2:348–354, 2002, quant-ph/0205107.

[169] D. Jonathan and M. B. Plenio. Minimal conditions for local pure-state entanglement manipulation. *Physical Review Letters*, 83:1455–1458, 1999, quant-ph/9903054.

[170] D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure quantum states. *Physical Review Letters*, 83:3566–3569, 1999, quant-ph/9905071.

[171] S. Karnas and M. Lewenstein. Separable approximations of density matrices of composite quantum systems. *Journal of Physics A: Mathematical and General*, 34:6919–6937, 2001, quant-ph/0011066.

[172] A. Kent. Entangled mixed states and local purification. *Physical Review Letters*, 81:2839–2841, 1998, quant-ph/9805088.

[173] A. Kent, N. Linden, and S. Massar. Optimal entanglement enhancement for mixed states. *Physical Review Letters*, 83:2656–2659, 1999, quant-ph/9902022.

[174] M. Keyl. Fundamentals of quantum information theory. *Physics Reports*, 369: 431–548, 2002, quant-ph/0202122.

[175] S. Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17(1):59–87, 1967.

[176] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein. Separability in $2 \otimes N$ composite quantum systems. *Physical Review A*, 61:062302, 2000, quant-ph/9912010.

[177] B. Kraus, M. Lewenstein, and J. I. Cirac. Characterization of distillable and activable states using entanglement witnesses. *Physical Review A*, 65:042327, 2002, quant-ph/0110174.

[178] K. Kraus. *States, Effects and Operations*. Lecture Notes in Physics. Springer, Berlin, Heidelberg, 1983.

[179] L. Labuschagne, W. Majewski, and M. Marciniak. On k-decomposability of positive maps. 2003, math-ph/0306017.

[180] M. Lamehi-Rachti and W. Mittig. Quantum mechanics and hidden variables: A test of Bell's inequality by the measurement of the spin correlation in low-energy proton-proton scattering. *Physical Review D*, 14:2543–2555, 1976.

[181] P. D. Lax. *Functional Analysis*. Wiley, 2002.

[182] M. Lewenstein and A. Sanpera. Separability and entanglement of composite quantum systems. *Physical Review Letters*, 80:2261–2264, 1998, quant-ph/9707043.

[183] M. Lewenstein, J. I. Cirac, and S. Karnas. Separability and entanglement in $2 \otimes N$ composite quantum systems. 1999, quant-ph/9903012.

[184] M. Lewenstein, D. Bruß, J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, and R. Tarrach. Separability and distillability in composite quantum systems – a primer –. *Journal of Modern Optics*, 47:2481–2499, 2000, quant-ph/0006064.

[185] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki. Optimization of entanglement witness. *Physical Review A*, 62:052310, 2000, quant-ph/0005014.

[186] M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac. Characterization of separable states and entanglement witness. *Physical Review A*, 63:044304, 2000, quant-ph/0005112.

[187] C.-K. Li and H. J. Woerdeman. Special classes of positive and completely positive maps. *Linear Algebra and its Applications*, 255:247–258, 1997.

[188] N. Linden and S. Popescu. Bound entanglement and teleportation. *Physical Review A*, 59:137–140, 1999, quant-ph/9807069.

[189] N. Linden, S. Massar, and S. Popescu. Purifying noisy entanglement requires collective measurements. *Physical Review Letters*, 81:3279–3282, 1998, quant-ph/9805001.

[190] H.-K. Lo and S. Popescu. Concentrating entanglement by local actions—beyond mean values. *Physical Review A*, 63:022301, 1997, quant-ph/9707038.

[191] H.-K. Lo and S. Popescu. Classical communication cost of entanglement manipulation: is entanglement an interconvertible resource? *Physical Review Letters*, 83:1459–1462, 1999, quant-ph/9902045.

[192] R. B. Lockhart and M. J. Steiner. Preserving entanglement under decoherence and sandwiching all separable states. *Physical Review A*, 65:022107, 2002, quant-ph/0009090.

[193] R. B. Lockhart, M. J. Steiner, and K. Gerlach. Geometry and product states. *Quantum Information and Computation*, 2:333–347, 2002, quant-ph/0010013.

[194] C. Macchiavello. On the analytical convergence of the qpa procedure. *Physics Letters A*, 246:385–388, 1998, quant-ph/9807074.

[195] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. Entanglement of orbital angular momentum states of photons. *Nature*, 412:313–316, 2001, quant-ph/0104070.

[196] W. A. Majewski. Some remarks on separability of states. 2000, quant-ph/0003007.

[197] W. A. Majewski. Positive maps, states, entanglement and all that; some old and new problems. 2004, quant-ph/0411043.

[198] W. A. Majewski. On positive maps, entanglement and quantization. *Open Systems and Information Dynamics*, 11:43–52, 2004, quant-ph/0404030.

[199] W. A. Majewski and M. Marciniak. On a characterization of positive maps. *Journal of Physics A: Mathematical and General*, 34:5863–5874, 2001.

[200] W. A. Majewski and M. Marciniak. *k*-decomposability of positive maps. 2004, quant-ph/0411035.

[201] E. N. Maneva and J. A. Smolin. Improved two-party and multi-party purification protocols. In S. J. Lomonaco and H. E. Brandt, editors, *AMS Contemporary Mathematics Series: Quantum Computation and Quantum Information*, volume 305, pages 203–212. American Mathematical Society, 2000.

[202] M. A. Martín-Delgado and M. Navascués. Distillation protocols for mixed states of multilevel qubits and the quantum renormalisation group. *European Physics Journal D*, 27:169–180, 2003, quant-ph/0301099.

[203] L. Masanes. All entangled states are useful for information processing. *Physical Review Letters*, 96:150501, 2006, quant-ph/0508071.

[204] L. Masanes. Useful entanglement can be extracted from all nonseparable states. 2005, quant-ph/0510188.

[205] K. Matsumoto and M. Hayashi. Universal distortion-free entanglement concentration. 2005, quant-ph/0509140.

[206] K. Matsumoto and F. Yura. Entanglement cost of antisymmetric states and additivity of capacity of some quantum channels. *Journal of Physics A: Mathematical and General*, 37:L167–L171, 2004, quant-ph/0306009.

[207] K. Matsumoto, T. Shimono, and A. Winter. Remarks on additivity of the Holevo channel capacity and of the entanglement of formation. *Communications in Mathematical Physics*, 246:427–442, 2004, quant-ph/0206148.

[208] R. Matsumoto. Conversion of a general quantum stabilizer code to an entanglement distillation protocol. *Journal of Physics A: Mathematical and General*, 36: 8113–8127, 2003, quant-ph/0209091.

[209] N. Metwally. A more efficient entanglement purification. *Physical Review A*, 66: 054302, 2001, quant-ph/0109051.

[210] N. Metwally and A.-S. Obada. More efficient purifying sheme via controlled-controlled NOT gate. *Physics Letters A*, 352:45–48, 2006.

[211] F. Morikoshi. Recovery of entanglement lost in entanglement manipulation. *Physical Review Letters*, 84:3189, 2000, quant-ph/9911019.

[212] F. Morikoshi and M. Koashi. Deterministic entanglement concentration. *Physical Review A*, 64:022319, 2001, quant-ph/0107120.

[213] M. A. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83:436–439, 1999, quant-ph/9811053.

[214] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[215] M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum. Information-theoretic approach to quantum error correction and reversible measurement. *Proceedings of the Royal Society London A*, 454:277–304, 1998, quant-ph/9706064.

[216] T. Opatrný and G. Kurizki. Optimization approach to entanglement distillation. *Physical Review A*, 60(1):167–172, 1999, quant-ph/9811090.

[217] H. Osaka. Indecomposable positive maps in low dimensional matrix algebras. *Linear Algebra and its Applications*, 153:73–83, 1991.

[218] C. J. Oxenrider and R. D. Hill. On the matrix reorderings Γ and Ψ. *Linear Algebra and its Applications*, 69:205–212, 1985.

[219] M. Ozawa. Entanglement measures and the Hilbert-Schmidt distance. *Physics Letters A*, 268:158–160, 2000, quant-ph/0002036.

[220] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger. Experimental entanglement swapping: entangling photons that never interacted. *Physical Review Letters*, 80:3891–3894, 1998.

[221] N. Paunković, Y. Omar, S. Bose, and V. Vedral. Entanglement concentration using quantum statistics. *Physical Review Letters*, 88:187903, 2002, quant-ph/0112004.

[222] A. Peres. *Quantum theory: concepts and methods*. Kluwer Academic Publishers, Dordrecht, 1993.

[223] A. Peres. Separability criterion for density matrices. *Physical Review Letters*, 77: 1413–1415, 1996, quant-ph/9604005.

[224] A. Peres. Collective tests for quantum nonlocality. *Physical Review A*, 54:2685, 1996, quant-ph/9603023, quant-ph/9609016.

[225] A. Peres. All the Bell inequalities. *Foundation of Physics*, 29:589–614, 1999, quant-ph/9807017.

[226] M. Piani. A class of $2^N \times 2^N$ bound entangled states revealed by non-decomposable maps. *Physical Review A*, 73:012345, 2006, quant-ph/0411098.

[227] M. Piani and C. E. Mora. Class of PPT bound entangled states associated to almost any set of pure entangled states. 2006, quant-ph/0607061.

[228] A. O. Pittenger. Unextendible product bases and the construction of inseparable states. *Linear Algebra and its Applications*, 359:235–248, 2003, quant-ph/0208028.

[229] M. B. Plenio. The logarithmic negativity: A full entanglement monotone that is not convex. *Physical Review Letters*, 95:090503, 2005, quant-ph/0505071.

[230] M. B. Plenio and S. Virmani. An introduction to entanglement measures. 2005, quant-ph/0504163.

[231] M. B. Plenio, S. Virmani, and P. Papadopoulos. Operator monotones, the reduction criterion and the relative entropy. *Journal of Physics A: Mathematical and General*, 33:L193–L197, 2000, quant-ph/0002075.

[232] J. A. Poluikis and R. D. Hill. Completely positive and Hermitian preserving linear transformations. *Linear Algebra and its Applications*, 35:1–10, 1981.

[233] S. Popescu. Bell's inequalities versus teleportation: what is nonlocality? *Physical Review Letters*, 72(6):797–799, 1994.

[234] S. Popescu. Bell's inequalities and density matrices: revealing 'hidden' nonlocality. *Physical Review Letters*, 74(14):2619–2622, 1995, quant-ph/9502005.

[235] S. Popescu and D. Rohrlich. Generic quantum nonlocality. *Physics Letters A*, 166:293–297, 1992.

[236] S. Popescu and D. Rohrlich. Thermodynamics and the measure of entanglement. *Physical Review A*, 56:3319–3321(R), 1997, quant-ph/9610044.

[237] M. Poźniak, K. Życzkowski, and M. Kuś. Composed ensembles of random unitary matrices. *Journal of Physics A*, 31:1059–1071, 1998, chao-dyn/9707006.

[238] E. M. Rains. A semidefinite program for distillable entanglement. *IEEE Transactions on Information Theory*, 47:2921–2933, 2000, quant-ph/0008047.

[239] E. M. Rains. Erratum: Bound on distillable entanglement. *Physical Review A*, 63:019902(E), 2000, quant-ph/9809082v2.

[240] E. M. Rains. Entanglement purification via separable superoperators. 1997, quant-ph/9707002.

[241] E. M. Rains. Bound on distillable entanglement. *Physical Review A*, 60:179–184, 1999, quant-ph/9809082v1.

[242] E. M. Rains. Rigorous treatment of distillable entanglement. *Physical Review A*, 60(1):173–178, 1999, quant-ph/9809078.

[243] J. Rarity and P. Tapster. Experimental violation of Bell's inequality based on phase and momentum. *Physical Review Letters*, 64:2495–2498, 1990.

[244] M. Redhead. *Incompletness, Nonlocality and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics.* Clarendon Press, Oxford, 1986.

[245] B. Reznick. Some concrete aspects of Hilbert's 17th problem. *Contemporary Mathematics*, 253:251–272, 2000.

[246] A. G. Robertson. Positive projections on C^*-algebra and an extremal positive map. *Journal of the London Mathematical Society*, 32:133–140, 1985.

[247] R. T. Rockafellar. *Convex Analysis.* Princeton University Press, 1970.

[248] M. Rowe, D. Kielpinski, V. Meyer, C. Sackett, W. Itano, C. Monroe, and D. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409:791–794, 2001.

[249] O. Rudolph. A separability criterion for density operators. *Journal of Physics A: Mathematical and General*, 33:3951–3955, 2000, quant-ph/0002026.

[250] O. Rudolph. A new class of entanglement measures. *Journal of Mathematical Physics*, 42:5306–5314, 2001, quant-ph/0005011.

[251] O. Rudolph. Further results on the cross norm criterion for separability. 2002, quant-ph/0202121.

[252] O. Rudolph. A note on "a matrix realignment method for recognizing entanglement" quant-ph/0205017 v1. 2002, quant-ph/0205054.

[253] O. Rudolph. Some properties of the computable cross norm criterion for separability. *Physical Review A*, 67:032312, 2003, quant-ph/0212047.

[254] O. Rudolph. Computable cross-norm criterion for separability. *Letters in Mathematical Physics*, 70:57–64, 2004.

[255] M. B. Ruskai. Inequalities for quantum entropy: a review with conditions for equality. *Journal of Mathematical Physics*, 43:4358–4375, 2002, quant-ph/0205064.

[256] M. B. Ruskai. Qubit entanglement breaking channels. *Reviews of Mathematical Physics*, 15:643–662, 2003, quant-ph/0302032.

[257] A. Sanpera, D. Bruß, and M. Lewenstein. Schmidt number witnesses and bound entanglement. *Physical Review A*, 63:050301(R), 2001, quant-ph/0009109.

[258] R. Schatten. *Norm ideals of completely continuous operators.* Springer, Berlin, Heidelberg, 2nd edition, 1970.

[259] E. Schmidt. Zur Theorie der linearen und nichtlinearen Integralgleichungen. *Mathematische Annalen*, 63:433–476, 1907.

[260] E. Schrödinger. Discussion of probability distributions between separated systems. *Proceedings of the Cambridge Philosophical Society*, 31:555–563, 1935.

[261] B. Schumacher and M. D. Westmoreland. Relative entropy in quantum information theory. In S. J. Lomonaco and H. E. Brandt, editors, *AMS Contemporary Mathematics Series: Quantum Computation and Quantum Information*, volume 305, pages 265–290. American Mathematical Society, 2000.

[262] A. Sen(De), U. Sen, and M. Lewenstein. Distillation protocols that involve local distinguishing: composing upper and lower bounds on locally accessible information. 2005, quant-ph/0505137.

[263] A. Sen(De), U. Sen, M. Lewenstein, and A. Sanpera. Lectures on quantum information. Chapter 1: The separability problem. 2005, quant-ph/0508032.

[264] B.-S. Shi, Y.-K. Jiang, and G.-C. Guo. Optimal entanglement purification via entanglement swapping. *Physical Review A*, 62:054301, 2000, quant-ph/0005125.

[265] T. Shimono. Lower bound for entanglement cost of antisymmetric states. 2002, quant-ph/0203039.

[266] A. Shimony. Degree of entanglement. *Annals New York Academy of Sciences*, 755:675–678, 1995.

[267] P. W. Shor. Additivity of the classical capacity of entanglement-breaking quantum channels. *Journal of Mathematical Physics*, 43:4334–4340, 2002, quant-ph/0201149.

[268] P. W. Shor. Equivalence of additivity questions in quantum information theory. *Communications in Mathematical Physics*, 246:453–472, 2004, quant-ph/0305035.

[269] P. W. Shor and J. A. Smolin. Quantum error-correcting codes need not completely reveal the error syndrome. 1996, quant-ph/9604006.

[270] P. W. Shor, J. A. Smolin, and B. M. Terhal. Nonadditivity of bipartite distillable entanglement follows from conjecture on bound entangled Werner states. *Physical Review Letters*, 86:2681–2684, 2001, quant-ph/0010054.

[271] P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Superactivation of bound entanglement. *Physical Review Letters*, 90:107901, 2003, quant-ph/0005117.

[272] N. J. A. Sloane. The on-line encyclopedia of integer published electronically at: http://www.research.att.com/~njas/sequences/.

[273] J. A. Smolin. A four-party unlockable bound-entangled state. *Physical Review A*, 63:032306, 2000, quant-ph/0001001.

[274] M. Steiner. Generalised robustness of entanglement. *Physical Review A*, 67: 054305, 2003, quant-ph/0304009.

[275] G. W. Stewart. The efficient generation of random orthogonal matrices with an application to condition estimators. *SIAM Journal of Numerical Analysis*, 17: 403–409, 1980.

[276] W. F. Stinespring. Positive functions on C^*-algebras. *Proceedings of the American Mathematical Society*, 6:211–216, 1955.

[277] E. Størmer. Positive linear maps of operator algebras. *Acta Mathematica*, 110: 233–278, 1963.

[278] E. Størmer. Decomposable positive maps on C^*-algebras. *Proceedings of the American Mathematical Society*, 86:402–404, 1982.

[279] A. Sudbery. The power of entanglement. Plenary lecture at the Fourth International Symposium on Quantum Theory and Symmetries, Varna, Bulgaria, 16 August 2005, 2005.

[280] A. Sudbery. Private communication, 2006.

[281] T. Takasaki and J. Tomiyama. On the geometry of positive maps in matrix algebras. *Mathematische Zeitschrift*, 184:101–108, 1983.

[282] W.S. Tang. On positive linear maps between matrix algebras. *Linear Algebra and its Applications*, 79:33–44, 1986.

[283] B. M. Terhal. Bell inequalities and the separability criterion. *Physics Letters A*, 217:319–326, 2000, quant-ph/9911057.

[284] B. M. Terhal. Detecting quantum entanglement. *Theoretical Computer Science*, 287:313–335, 2001, quant-ph/0101032.

[285] B. M. Terhal. A family of indecomposable positive linear maps based on entangled quantum states. *Linear Algebra and its Applications*, 323:61–73, 2001, quant-ph/9810091.

[286] B. M. Terhal and P. Horodecki. A Schmidt number for density matrices. *Physical Review A*, 61:040301(R), 2000, quant-ph/9911117.

[287] B. M. Terhal and K. G. V. Vollbrecht. The entanglement of formation for isotropic states. *Physical Review Letters*, 85:2625–2628, 2000, quant-ph/0005062.

[288] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of Bell inequalities by photons more than 10 km apart. *Physical Review Letters*, 81:3563–3566, 1998, quant-ph/9806043.

[289] J. Tomiyama. On the geometry of positive maps in matrix algebras. II. *Linear Algebra and its Applications*, 69:169–177, 1985.

[290] W. van Dam and P. Hayden. Embezzling entangled quantum states. *Physical Review A*, 67:060302(R), 2003, quant-ph/0201041.

[291] V. Vedral. The role of relative entropy in quantum information theory. *Reviews of Modern Physics*, 74:197–234, 2002, quant-ph/0102094.

[292] V. Vedral. On bound entanglement assisted distillation. *Physics Letters A*, 262: 121–124, 1999, quant-ph/9908047.

[293] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3):1619–1633, 1998, quant-ph/9707035.

[294] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Physical Review Letters*, 78(12):2275–2279, 1997, quant-ph/9702027.

[295] F. Verstraete. *A study of entanglement in quantum information theory.* PhD thesis, Katholieke Universiteit Leuven, 2002.

[296] F. Verstraete and H. Verschelde. On quantum channels. 2002, quant-ph/0202124.

[297] F. Verstraete and H. Verschelde. Optimal teleportation with a mixed state of two qubits. *Physical Review Letters*, 90:097901, 2003, quant-ph/0303007.

[298] F. Verstraete, J. Dehaene, and B. De Moor. Local filtering operations on two qubits. *Physical Review A*, 64:010101(R), 2001, quant-ph/0011111.

[299] G. Vidal. Entanglement monotones. *Journal of Modern Optics*, 47:355–376, 2000, quant-ph/9807077.

[300] G. Vidal. On the continuity of asymptotic measures of entanglement. quant-ph/0203107.

[301] G. Vidal. Entanglement of pure states for a single copy. *Physical Review Letters*, 83(5):1046–1049, 1999, quant-ph/9902033.

[302] G. Vidal and J. I. Cirac. Irreversibility in asymptotic manipulations of entanglement. *Physical Review Letters*, 86:5803–5806, 2001, quant-ph/0102036.

[303] G. Vidal and J. I. Cirac. When only two thirds of the entanglement can be distilled. *Physical Review A*, 65:012323, 2002, quant-ph/0107051.

[304] G. Vidal and R. Tarrach. Robustness of entanglement. *Physical Review A*, 59: 141–155, 1999, quant-ph/9806094.

[305] G. Vidal and R. F. Werner. A computable measure of entanglement. *Physical Review A*, 65:032314, 2002, quant-ph/0102117.

[306] G. Vidal, D. Jonathan, and M. A. Nielsen. Approximate transformations and robust manipulation of bipartite pure state entanglement. *Physical Review A*, 62:012304, 2000, quant-ph/9910099.

[307] G. Vidal, W. Dür, and J. I. Cirac. Entanglement cost of mixed states. *Physical Review Letters*, 89:027901, 2002, quant-ph/0112131.

[308] K. G. H. Vollbrecht and F. Verstraete. Interpolation of recurrence and hashing entanglement distillation protocols. *Physical Review A*, 71:062325, 2005, quant-ph/0404111.

[309] K. G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *Physical Review A*, 64:062307, 2001, quant-ph/0010095.

[310] K. G. H. Vollbrecht and M. M. Wolf. Activating NPT distillation with an infinitesimal amount of bound entanglement. *Physical Review Letters*, 88:247901, 2002, quant-ph/0201103.

[311] K. G. H. Vollbrecht and M. M. Wolf. Efficient distillation beyond qubits. *Physical Review A*, 67:012303, 2003, quant-ph/0208152.

[312] K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf. On the irreversibility of entanglement distillation. *Physical Review A*, 69:062304, 2004, quant-ph/0301072.

[313] J. Walgate, A. J. Short, L. Hardy, and V. Vedral. Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 85:4972–4975, 2000, quant-ph/0007098.

[314] X. Wang and P. Zanardi. Quantum entanglement of unitary operators on bipartite systems. *Physical Review A*, 66:044303, 2002, quant-ph/0207007.

[315] S. Watanabe, R. Matsumoto, and T. Uyematsu. Improvement of stabilizer based entanglement distillation protocols by encoding operators. *Journal of Physics A: Mathematical and General*, 39:4273–4290, 2006, quant-ph/0506054.

[316] J. Watrous. On the number of copies required for entanglement distillation. *Physical Review Letters*, 93:010502, 2004, quant-ph/0312123.

[317] T.-C. Wei and P. M. Goldbart. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Physical Review A*, 68: 042307, 2003, quant-ph/0307219.

[318] T.-C. Wei, J. B. Altepeter, P. M. Goldbart, and W. J. Munro. Measures of entanglement in multipartite bound entangled states. *Physical Review A*, 70: 022322, 2004, quant-ph/0308031.

[319] T.-C. Wei, M. Ericsson, P. M. Goldbart, and W. J. Munro. Connections between relative entropy of entanglement and geometric measure of entanglement. *Quantum Information and Computation*, 4:252–272, 2004, quant-ph/0405002.

[320] T. Wellens and M. Kuś. Separable approximation for mixed state of composite quantum systems. *Physical Review A*, 65:052302, 2001, quant-ph/0104098.

[321] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40:4277–4281, 1989.

[322] R. F. Werner and M. M. Wolf. Bound entangled Gaussian states. *Physical Review Letters*, 86:3658–3661, 2001, quant-ph/0009118.

[323] C. Witte and M. Trucks. A new entanglement measure induced by the Hilbert-Schmidt norm. *Physics Letters A*, 257:14–20, 1999, quant-ph/9811027.

[324] P. Wocjan and M. Horodecki. Characterization of combinatorically independent permutation separability criteria. *Open Systems and Information Dynamics*, 12: 331–345, 2005, quant-ph/0503129.

[325] H. J. Woerdeman. Checking $2 \times M$ quantum separability via semidefinite programming. *Physical Review A*, 67:010303(R), 2003, quant-ph/0301058.

[326] W. K. Wootters. Entanglement of formation and concurrence. *Quantum Information and Computation*, 1:27–44, 2001.

[327] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80:2245–2248, 1997, quant-ph/9709029.

[328] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Reports on Mathematical Physics*, 10:165–183, 1976.

[329] S. Wu and Y. Zhang. Calculating the relative entropy of entanglement. 2000, quant-ph/0004018.

[330] D. Yang and Y.-X. Chen. Mixture of multiple copies of maximally entangled states is quasi-pure. *Physical Review A*, 69:024302, 2004, quant-ph/0304194.

[331] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke. Irreversibility for all bound entangled states. *Physical Review Letters*, 95:190501, 2005, quant-ph/0506138.

[332] S. Yu and N.l. Liu. Entanglement detection by local orthogonal observables. *Physical Review Letters*, 95:150504, 2005, quant-ph/0412220.

[333] F. Yura. Entanglement cost of three-level antisymmetric states. *Journal of Physics A: Mathematical and General*, 36:L237–L242, 2003, quant-ph/0302163.

[334] B. Yurke and D. Stoler. Bell's-inequality experiments using independent-particle sources. *Physical Review A*, 46:2229–2234, 1992.

[335] B. Yurke and D. Stoler. Einstein-Podolsky-Rosen effects from independent particle sources. *Physical Review Letters*, 68:1251–1254, 1992.

[336] P. Zanardi. Entanglement of quantum evolutions. *Physical Review A*, 63:040304(R), 2001, quant-ph/0010074.

[337] P. Zanardi, C. Zalka, and L. Faoro. On the entangling power of quantum evolutions. *Physical Review A*, 62:030301(R), 2000, quant-ph/0005031.

[338] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. Event-Ready-Detectors: Bell experiment via entanglement swapping. *Physical Review Letters*, 71:4287–4290, 1993.

[339] K. Życzkowski. Volume of the set of mixed entangled states II. *Physical Review A*, 60:3496–3507, 1999, quant-ph/9902050.

[340] K. Życzkowski and I. Bengtsson. On duality between quantum maps and quantum states. *Open Systems and Information Dynamics*, 11:3–42, 2004, quant-ph/0401119.

[341] K. Życzkowski and M. Kuś. Random unitary matrices. *Journal of Physics A: Mathematical and General*, 27:4235–4245, 1994.

[342] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. On the volume of the set of mixed entangled states. *Physical Review A*, 58:883–892, 1998, quant-ph/9804024.